RODO w PR

Jak wdrożyć RODO w Twojej firmie

cz. 1

Prowly · JSLEGAL Jankowski & Stroiński · Fundacja Panoptykon · Szapiro | Schwann Public Relations

RODO – to hasło od kilku miesięcy spędza sen z powiek wielu przedsiębiorcom

Branże *public relations* i marketingowa nie są żadnymi wyjątkami. Idziemy o zakład, że zastawiasz się, czy podejmujesz odpowiednie działania i czy zdążysz na czas przygotować się do nowych zasad gry. Jak większość, możesz mieć problem z interpretacją nowych przepisów.

Dlatego przygotowaliśmy e-book, który pomoże krok po kroku wdrożyć RODO/GDPR w Twoim biznesie. Podzieliliśmy go na dwie części – w każdej znajdziesz ujęcie teoretyczne i praktyczne problemu.

W e-booku podpowiadamy, kogo dokładnie dotyczy RODO i jakie uprawnienia przewiduje dla osób, których dane są przetwarzane.

Wyjaśniamy, jakie obowiązki informacyjne i organizacyjne na Tobie ciążą oraz jak możesz przeprowadzić audyt i zaprojektować wewnętrzne procedury w swojej firmie. Pomagamy sprawdzić, czy prawidłowo przetwarzasz dane osobowe, i rekomendujemy najlepsze rozwiązania. Analizujemy klauzule, na które powołują się inni, i podpowiadamy, jak monitorować i ewidencjonować procesy. Wreszcie pokazujemy, jak dwie agencje z naszego rynku już wdrożyły RODO, bo wierzymy, że dobrymi praktykami należy się dzielić. Tak, jest tego sporo, ale staraliśmy się, by materiał był solidny i kompleksowy.

Wykorzystaj tę wiedzę i nie daj się zastraszyć!

Edyta Kowal
Content Marketing Manager & Editor,
Prowly

Karol Schwann
Director of Operations,
Szapiro Schwann Public Relations

Co znajdziesz w naszym e-booku?

Poniższa plansza stanowi jednocześnie gotowy do wdrożenia plan przygotowania Twojej firmy na RODO/GDPR oraz spis treści, które prezentujemy w e-booku.

Kliknij w wybraną sekcję, by przenieść się do omówienia tego konkretnego problemu. Wyszarzone elementy planszy omówimy w drugiej części e-booka (dostaniesz ją na swoją skrzynkę za kilka dni). Znajdziesz w niej *case studies* dwóch agencji, które są już przygotowane pod kątem RODO. Przyjemnej lektury!

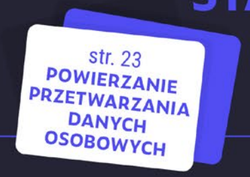
Fundamentalne zasady przetwarzania danych str. 5

Nowe (i stare) uprawnienia osób, których dane dotyczą str.7

Kogo dotyczy RODO str. 8

Nowe regulacje wprowadzone przez RODO str. 10

START



Analiza	Analiza	Analiza	Analiza przekazywania danych podmiotom trzecim		Analiza pozyskiwania zgód		Oceny ryzyka	Przygotowanie rejestru czynności przetwarzania danych osobowych	
Ocena prawidłowości przetwarzania danych osobowch	Ocena prawidłowości przetwarzania danych osobowych		Analiza stosowanych rozwiązań	Analiza podstaw przekazywania poza EOG	Analiza stosowanych wzorów		*Case study*	*Case study*	
Rekomendacja w obszarze sposobu przetwarzania danych osobowych	Rekomendacja w obszarze sposobu przetwarzania danych osobowych	Modyfikacje	Opracowanie nowego wzoru umowy	Aktualizacja dokumentacji	Przygotowanie nowych wzorów	Pozyskanie na nowo nieprawidłowo pozyskanych zgód	Opracowanie procedury i wzoru oceny skutków		

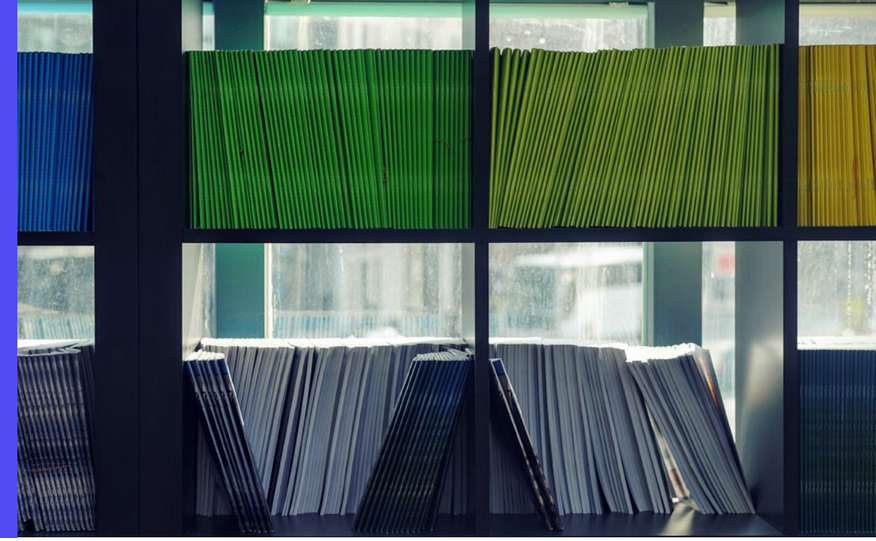
AKTUALIZACJA POLITYKI OCHRONY DANYCH OSOBOWYCH

Wdrożenie zmian	Wdrożenie zmian	Wdrożenie modyfikacji	Wdrożenie nowego wzoru umowy	Wdrożenie dokumentacji	Wdrożenie nowych wzorów		Wdrożenie procedur	Wdrożenie rejestru

MONITOROWANIE I EWIDENCJONOWANIE PROCESÓW; WPROWADZANIE MODYFIKACJI W MIARĘ POTRZEBY

META

Fundamentalne zasady **przetwarzania danych**



FUNDACJA PANOPTYKON

Rewolucja czy lifting dotychczas obowiązujących zasad, czyli co zmienia RODO

Pełne wdrożenie RODO może się okazać wyzwaniem dla wielu firm, szczególnie tych, które wykorzystują dane osobowe na masową skalę. Tego procesu nie należy jednak utożsamiać z samymi obciążeniami. To także szansa na uproszczenie procedur oraz zbudowanie z klientami relacji opartej na zaufaniu i zrozumieniu ich potrzeb związanych z ochroną prywatności.

Przetwarzanie danych jest traktowane w RODO jako proces, który z definicji stwarza pewne ryzyko dla praw i wolności osób fizycznych. Nie oznacza to, że danych osobowych nie można wykorzystywać. Owszem, możesz to robić, ale tylko w ściśle określonych prawem ramach wyznaczonych przez tzw. zasady przetwarzania danych (por. kolejny punkt). W praktyce oznacza to, że każdy, kto zamierza podjąć taką działalność, już na wstępie powinien się zmierzyć z konkretną listą pytań:

- Jakie rodzaje danych będą przetwarzane, w jakich celach i w jaki sposób?
- Czy przetwarzanie wszystkich tych informacji jest niezbędne i proporcjonalne?
- Czy jesteś w stanie określić podstawy prawne ich przetwarzania?
- Czy – mimo formalnego spełnienia obowiązków prawnych – z przetwarzaniem tych danych może się wiązać ryzyko dla osób, których one dotyczą (tj. określone zagrożenia)?
- Czy potrafisz zidentyfikować rodzaje, źródła i poziom tych zagrożeń?
- Czy potrafisz tym zagrożeniom zaradzić, a przynajmniej je zminimalizować?

Zmierzenie się z wymogami RODO warto zacząć od rzetelnego zmapowania źródeł i przepływów danych, następnie – ocenić legalność ich przetwarzania, a dopiero w kolejnym kroku analizować możliwe konsekwencje takiego działania dla podmiotów danych (ocena ryzyka sensu *stricto*). Jeśli już na pierwszym etapie pojawią się jakieś wątpliwości, zastanów się, czy rzeczywiście warto iść dalej. Zgodność przetwarzania danych z RODO weryfikuje się nie tylko raz, ale cyklicznie, a weryfikacja ta nie ma linearnego charakteru. Czasem (np. w przypadku zdiagnozowania wysokiego ryzyka związanego z przetwarzaniem danych) RODO nakazuje powtórzenie pewnych czynności. Każdy etap rozwija się w kolejny proces, co powoduje, że mamy do czynienia ze złożoną konstrukcją.

Kolejne rozdziały tego opracowania zawierają praktyczne wskazówki, jak się zmierzyć z poszczególnymi etapami i procesami.

T

Ugruntowane zasady

Mimo dużej elastyczności, jaką administratorom danych daje RODO, pewne elementy są stałe. Na poziomie podstawowych zasad przetwarzania danych i konkretnych praw przysługujących osobom, których dane dotyczą, rozporządzenie nie wprowadza rewolucji: to raczej lifting dotychczas obowiązujących przepisów.

Jeśli masz jakiekolwiek wcześniejsze doświadczenia związane z ochroną danych, te przepisy wydadzą Ci się znajome.
Oto podstawowe zasady przetwarzania danych osobowych:

- legalność,
- ograniczenie celem,
- adekwatność, niezbędność i minimalizacja,
- prawidłowość,
- maksymalny czas przetwarzania,
- poufność i integralność,
- przejrzystość*.

Te zasady to podstawowa check-lista każdego administratora. W praktyce musi się z nimi zmierzyć albo zarząd organizacji (firmy, instytucji publicznej), albo osoba przez ten zarząd oddelegowana (zgodnie z nowymi regułami będzie to inspektor ochrony danych).

Podstawowym obowiązkiem administratora jest zapewnienie przestrzegania tych zasad: zadbanie o to, by w organizacji nie było danych osobowych nieadekwatnych do celu, niepoprawnych, narażonych na ryzyko wycieku bądź przetwarzanych bez podstawy prawnej, w innym celu niż pierwotnie zakładany czy po prostu zbyt długo.

Logiczną konsekwencją zasad broniących dostępu do danych osobowych są – wynikające z nich bezpośrednio – prawa osób, których dane są przetwarzane. Jeśli administrator jest w stanie wykazać, że przetwarza dane zgodnie z zasadami, jakie przewiduje RODO, nie powinien mieć też żadnego problemu ze zrealizowaniem swoich obowiązków względem osób, których te dane dotyczą. Podążając za wewnętrzną logiką tej regulacji, można spojrzeć na prawa osób, których dane są przetwarzane, jako na drugi bastion chroniący przed ryzykownymi lub nielegalnymi praktykami. Jeśli fundamentalne zasady przetwarzania danych to granica, poza którą żaden administrator danych nie powinien wychodzić, prawa podmiotów danych to treść, bez której standard ochrony danych przewidziany w RODO byłby pusty.

* Na gruncie RODO przejrzystość jest traktowana jako bezwzględny warunek zgodności przetwarzania danych z prawem, podobnie jak pozostałe zasady. Jednak w praktyce trudno ją sprowadzić do twardego kryterium (jest/nie ma). Dlatego w tym przewodniku traktujemy ją jako standard, którego administrator powinien przestrzegać w relacji z podmiotami danych.

Nowe (i stare) **uprawnienia osób**, których dane dotyczą

FUNDACJA PANOPTYKON

Jakie uprawnienia przewiduje RODO dla osób, których dane są przetwarzane?

- Prawo do informacji o tym, jakie dane i w jakich celach są przetwarzane, a w przypadku zautomatyzowanego podejmowania decyzji (w tym profilowania) – także do informacji o zasadach ich podejmowania, znaczeniu i przewidywanych konsekwencjach takiego przetwarzania (zgodnie z art. 12, 13 i 14).
- Prawo do udostępniania i przeniesienia danych (zgodnie z art. 15 i 20).
- Prawo do poprawienia i usunięcia danych (zgodnie z art. 16 i 17).
- Prawo do wycofania zgody w każdym momencie, zgłoszenia sprzeciwu lub żądania ograniczenia przetwarzania danych (zgodnie z art. 7, 18 i 21).
- Prawo do ludzkiej interwencji i zakwestionowania decyzji w sytuacji, kiedy system mówi „nie” (zgodnie z art. 22).

Wśród tych praw trudno wskazać ważne i ważniejsze. Realne konsekwencje ich naruszenia mogą mieć różne znaczenie w zależności od kontekstu i sytuacji życiowej osoby, której dane dotyczą. Na przykład prawo poprawienia danych będzie miało inny wymiar w kontekście marketingowym (źle dopasowana reklama), a inny w relacji z bankiem czy państwem (kiedy w grę wchodzi błędna i wiążąca decyzja). A jednak trudno sobie wyobrazić sensowne żądanie sprostowania czy usunięcia danych albo zgłoszenie sprzeciwu wobec praktyk marketingowych bez wiedzy na temat tego, jakie dane rzeczywiście są przetwarzane. Dostęp do rzetelnych informacji ma kluczowe znaczenie w kontekście praktycznej możliwości zrealizowania pozostałych uprawnień. W tym sensie uprawnienia wynikające z art. 12–14 RODO są bazą i warunkiem umożliwiającym realizację pozostałych.

Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.

Więcej informacji na temat redagowania zgód znajdziesz na stronie 26

Europejski regulator traktuje z równą powagą naruszenie każdego z uprawnień, które wynikają z RODO (art. 12–20), i obwarowuje te naruszenia najpoważniejszymi sankcjami: administracyjnymi karami pieniężnymi w wysokości do 20 mln euro lub 4% globalnego obrotu.

Sprawdź, na jakie kary się narażasz

Kogo dotyczy **RODO**

JSLEGAL JANKOWSKI & STROIŃSKI

Rozporządzenie o ochronie danych osobowych (w dalszej części tekstu określane jako RODO lub rozporządzenie) spędza sen z powiek przedsiębiorcom, którzy z każdej strony zasypywani są informacjami o RODO i ciągłymi pytaniami, czy są już gotowi i czy wdrożyli nowe zasady. Z raportu Kantar Public, sporządzonego w grudniu 2017 roku dla Generalnego Inspektora Ochrony Danych Osobowych, wynika, że 24% badanych przedsiębiorców nie wie, od kiedy zaczną obowiązywać nowe przepisy, a aż 72% ankietowanych nie zna zakresu zmian wynikających z RODO. To pokazuje, jak wielu przedsiębiorców ma znikomą wiedzę na temat nowych przepisów.

Jeśli nadal się zastanawiasz, czy obowiązki wynikające z RODO dotyczą również Ciebie, musisz przeanalizować, jaki jest zakres i charakter Twojej działalności i czy prowadząc działalność gospodarczą lub świadcząc usługi osobiście, masz do czynienia z jakimikolwiek danymi osobowymi.

Niezależnie od tego, czy prowadzisz mikro- czy małe przedsiębiorstwo, część obowiązków, które wprowadza rozporządzenie, może dotyczyć również Ciebie, jeśli przetwarzasz dane osobowe osób fizycznych, np. pracowników, kandydatów, kontrahentów czy klientów.

Nowe rozporządzenie dotyczy każdego przedsiębiorcy, który prowadzi działalność w Unii Europejskiej, niezależnie od formy prawnej i rodzaju działalności. Dlatego warto sprawdzić, czy dokonujesz jakichkolwiek operacji na danych osobowych.

Według RODO dane osobowe to informacje o osobie, której dane dotyczą, oraz o osobie fizycznej, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji, identyfikatorze internetowym lub jednego bądź kilku szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dla przykładu, jeśli w ramach swojej działalności zatrudniasz choćby jednego pracownika lub zlecasz wykonanie usług lub dzieła osobie fizycznej, musisz mieć świadomość, że w związku z tą współpracą masz dostęp do danych osobowych tych osób i to jest już materią RODO.

Wdrożenie RODO będzie również obowiązkowe w sytuacji, kiedy prowadzisz jednoosobową działalność gospodarczą, w ramach której wykonujesz usługi osobiście i w celu wykonania usług zbierasz dane osobowe np. kontrahentów będących osobami fizycznymi lub prowadzących jednoosobową działalność gospodarczą, ponieważ dane tych przedsiębiorców na gruncie RODO uznaje się za dane osobowe.

Przetwarzać dane osobowe można jako administrator danych lub podmiot przetwarzający. Administratorem może być osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Np. szpital będzie administratorem

danych osobowych pacjentów, a wydawnictwo będzie administratorem danych osobowych swoich pracowników czy autorów, z którymi współpracuje. Zaś podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który działa na podstawie umowy z administratorem i przetwarza dane osobowe w jego imieniu. Takim podmiotem przetwarzającym będzie podmiot zewnętrzny, który wykonuje usługi na rzecz administratora, a podczas wykonywania tych usług przeprowadza operacje na danych osobowych, których administratorem jest zlecający, np. biuro księgowe. Upraszczając, można powiedzieć, że administratora danych poznamy po tym, że sam decyduje o celach i środkach przetwarzania – czyli nadzoruje przetwarzanie danych osobowych, wybiera cele, do których wykorzystuje dane osobowe, oraz środki techniczne, jakich używa do przetwarzania. Inaczej jest w wypadku podmiotu przetwarzającego, który przetwarza dane w celu narzuconym przez administratora i w jego imieniu.

Niekiedy co najmniej dwaj przedsiębiorcy przetwarzają dane osobowe we wspólnym celu, przez co na gruncie RODO powstanie stosunek współadministrowania. Jako współadministratorzy podmioty wspólnie określają cele i sposoby przetwarzania, a także wskazują zakres swojej odpowiedzialności. Taka sytuacja najczęściej może wystąpić podczas realizacji wspólnych projektów lub wykonywania usług przez kilku przedsiębiorców, lub w grupach kapitałowych.

Szersze definicje administratorów i współadministratorów podajemy na stronie 11

Wdrożenie nowych przepisów będzie również obowiązkiem podmiotu, który nie ma siedziby na terytorium Unii Europejskiej, ale wykonuje jakiekolwiek operacje na danych osobowych osób znajdujących się w UE, jeśli operacje te wiążą się ze sprzedażą towarów lub usług oraz monitorowaniem zachowania tych osób. RODO dotyczy również sytuacji, w której jednostka nie działa na obszarze UE, ale zgodnie z regulacjami międzynarodowymi obowiązuje w niej prawo UE – chodzi tu np. o konsulaty.

Rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną, jeśli nie ma to związku z jej działalnością zawodową lub handlową. Jako osoby fizyczne możemy spokojnie zbierać i przechowywać adresy oraz telefony członków rodziny i znajomych bez wdrażania RODO. Przetwarzanie danych osobowych osób zmarłych również będzie wyłączone spod nowych przepisów.

Nowe regulacje wprowadzone przez RODO

JSLEGAL JANKOWSKI & STROIŃSKI

RODO wprowadza wiele regulacji, które albo są całkowicie nowe (tj. nie były znane dotychczas obowiązującej ustawie o ochronie danych osobowych), albo nie są wprawdzie innowacyjne, ale zostały obwarowane poważnymi sankcjami za ich nieprzestrzeganie, więc siłą rzeczy stały się istotne dla wszystkich podmiotów zajmujących się przetwarzaniem danych. Dla administratora danych oraz podmiotu przetwarzającego w praktyce oznacza to konieczność realizacji dodatkowych obowiązków związanych z ochroną danych oraz implementację nowych procedur, które będą wprowadzały w życie te nowe RODO-regulacje na poziomie organizacji administratora.

Zobacz: ramka na stronie 15

Kwestię klauzul informacyjnych szerzej opisujemy na stronach 26-31

Poszerzone obowiązki informacyjne oraz organizacyjne

W ramach poszerzonego obowiązku informacyjnego podmiot przetwarzający dane będzie zobowiązany do przekazania osobie, której dane dotyczą, dużo szerszego zakresu informacji niż ten, który był wymagany przez dotychczas obowiązującą ustawę o ochronie danych. Osobie, której dane są lub będą przetwarzane, należy obecnie podać m.in. następujące informacje: dane kontaktowe Inspektora Ochrony Danych, wskazanie podstawy prawnej przetwarzania danych, informację o zamiarze przekazywania danych do państwa spoza EOG, wskazanie okresu, przez który dane będą przetwarzane, informację o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu, informację o prawach osoby, której dane dotyczą, oraz sposobie realizacji tych praw (w tym prawie do bycia zapomnianym, prawie skargi do organu nadzorczego, prawie do wyrażenia sprzeciwu itd.). Rzecz dotyczy więc w uproszczeniu konieczności rozbudowania klauzuli informacyjnej, która powinna być dostępna dla osoby, której dane dotyczą, tak by ta osoba mogła się z nią zapoznać w momencie, gdy jej dane są zbierane.

Jeśli chodzi o środki organizacyjne, RODO nakłada dodatkowo na podmiot przetwarzający dane:

a) obowiązek wdrożenia odpowiednich polityk ochrony danych (przy czym nie precyzuje, jakie mają to być dokumenty, o jakiej nazwie i o jakiej zawartości, pozostawiając tę kwestię do ustalenia podmiotowi przetwarzającemu dane),
b) obowiązek prowadzenia rejestru czynności przetwarzania danych,
c) obowiązek przeprowadzenia oceny skutków planowanych operacji przetwarzania danych

(przy czym obu tych ostatnich obowiązków nie musi wypełniać każdy podmiot przetwarzający, konieczność ich dopełnienia powstaje tylko w określonych – wskazanych w RODO – okolicznościach). Ponadto podmiot przetwarzający dane

powinien stosować zatwierdzone przez właściwe podmioty kodeksy postępowania lub mechanizmy certyfikacji (szeroka regulacja w zakresie tych nowych „instytucji" znajduje się w RODO), a także przetwarzać dane wyłącznie w zakresie, celu i czasie, które są niezbędne, i wdrażać stosowne środki bezpieczeństwa, w tym np. pseudonimizację danych, tworzenie kopii zapasowych itp.

Jak zostało wskazane powyżej, nie wszystkie z nowo wprowadzonych obowiązków organizacyjnych będą dotyczyć każdego podmiotu przetwarzającego dane. Część z nich zależy od rozmiaru przedsiębiorstwa podmiotu przetwarzającego dane, a także wolumenu i charakteru przetwarzanych przez ten podmiot danych.

Zmiana w relacjach między podmiotami przetwarzającymi dane osobowe (administrator, współadministrator, podmiot przetwarzający)

RODO wyróżnia trzy główne podmioty, które mogą przetwarzać dane osobowe. Są to administrator, podmiot przetwarzający oraz współadministratorzy.

Administratorem jest taki podmiot, który niekoniecznie sam przetwarza dane osobowe (bo np. zleca to innemu podmiotowi), ale decyduje o sposobach i celach przetwarzania tych danych. Te dwie przesłanki – decydowania o sposobie i decydowania o celu – wyróżniają administratora spośród innych podmiotów, które przetwarzają dane. Administrator więc nie musi być rzeczywiście w posiadaniu danych, nie musi nawet wykonywać na nich żadnej operacji, ale – jeśli jakiś podmiot wykonuje te czynności na jego rzecz – to robi to zawsze w taki sposób i w takim celu, jak poleci mu administrator. Na administratorze, jako dysponencie danych osobowych, spoczywa większość obowiązków wynikających z RODO, a dotyczących ochrony tych danych. To także do administratora mogą się zwracać w różnych kwestiach osoby, których danymi administruje.

Podmiotem przetwarzającym został w RODO nazwany ten właśnie podmiot, który na zlecenie administratora przetwarza dane, respektując sposoby i cele ich przetwarzania wskazane mu przez administratora. Jest więc on dysponentem danych (zarówno co do ich zawartości, jak i operacji, które mogą być na nich wykonywane) tylko w takim zakresie, jaki został mu przekazany przez administratora danych. Powierzenie przetwarzania danych osobowych musi nastąpić na piśmie w drodze umowy pomiędzy administratorem a podmiotem przetwarzającym, a umowa ta ma wskazywać wszystkie zasady dotyczące przetwarzania danych przez podmiot przetwarzający. Podmiot przetwarzający odpowiada wobec administratora za bezpieczeństwo danych w powierzonym mu zakresie, natomiast wobec osób, których dane dotyczą, odpowiedzialny jest administrator. Jeśli podmiot przetwarzający nie przestrzega przepisów RODO dotyczących ochrony danych, może go dotknąć jedna z kar przewidzianych przez RODO. Oznacza to, że podmiot przetwarzający musi także wdrożyć w swojej organizacji wszelkie środki niezbędne do zapewnienia odpowiedniego poziomu bezpieczeństwa danych (w tym np. jest zobowiązany prowadzić stosowny rejestr kategorii czynności przetwarzania), co więcej, ma obowiązek poddać się kontroli administratora w tym zakresie.

Zobacz: RODO a administracyjne kary pieniężne

Kolejnym przykładem współpracy dwóch (lub większej liczby) podmiotów w kwestii przetwarzania danych osobowych jest nowa instytucja wprowadzona przez RODO, czyli współadministrowanie. Zakłada ona, że wobec jednego zbioru danych dwa (lub więcej) podmioty wspólnie ustalają cele i sposoby ich przetwarzania. Podział obowiązków w ramach takiej współpracy współadministratorzy regulują w stosownej umowie zawartej pomiędzy sobą, która powinna określać m.in. zakres odpowiedzialności każdego ze współadministratorów dotyczącej wypełniania obowiązków z RODO, w tym w odniesieniu do wykonywania przysługujących jej praw przez osobę, której dane dotyczą. Zasadnicza treść uzgodnień pomiędzy współadministratorami powinna zostać udostępniona osobom, których dane przetwarzają, w ramach realizacji obowiązku informacyjnego.

Czasami dochodzi także do sytuacji, w której wobec jednego zbioru danych co do ich części o sposobach i celach ich przetwarzania będzie decydował jeden, a co do pozostałej części – drugi podmiot. Wówczas, jeśli sposoby i cele przetwarzania nie są wspólne, nie będziemy mówić o relacji współadministrowania, ale o dwóch oddzielnych administratorach danych, którzy w zakresie pochodzących z jednego zbioru danych, którymi sami administrują, mogą przekazywać je drugiemu podmiotowi w tej relacji na zasadzie powierzenia przetwarzania danych.

Automatyczne przetwarzanie i profilowanie

W zakresie automatycznego przetwarzania danych oraz profilowania RODO wprowadza obostrzenie związane ze stosowaniem tych operacji.

Profilowanie, które z dużymi emocjami wspomina się w kontekście regulacji RODO, polega na ocenie czynników osobowych danej jednostki i przewidywaniu jej zachowania. Nie jest to pojęcie całkiem nowe. Poprzednio obowiązująca ustawa o ochronie danych osobowych także przewidywała prawo do ochrony przed poddawaniem jednostki zautomatyzowanemu procesowi decyzyjnemu, przy czym – jak w wielu innych przypadkach – nie przewidywała za naruszenie przepisów dotyczących tej instytucji tak wysokich i dotkliwych kar, jak RODO.

Zgodnie z RODO automatycznym przetwarzaniem jest każde przetwarzanie danych osobowych, które opiera się na działaniu jakiegoś automatu (maszyny), tj. dokonuje się go bez udziału czynnika ludzkiego. Profilowanie natomiast, będące jedną z form automatycznego przetwarzania, jest sposobem przetwarzania danych, na którym może bazować decyzja podejmowana przez podmiot przetwarzający dane. Profilowanie zawsze jest procesem automatycznym, polega na wykorzystaniu danych osobowych, a jego celem jest ocena czynników osobowych danej jednostki. Jeśli w ramach procesu brakuje któregokolwiek z tych trzech czynników, nie możemy mówić o profilowaniu w świetle RODO.

Profilowanie jest bardzo atrakcyjne dla branży marketingowej – pozwala ono w łatwy sposób przeanalizować wiele danych, które są szeroko dostępne w internecie, i za pomocą automatów znaleźć korelację między tymi danymi oraz stworzyć stosowne powiązania. To z kolei umożliwia tworzenie profili i podejmowanie automatycznych decyzji. Pozytywnym skutkiem profilowania jest łatwe i szybkie dopasowanie produktów lub usług do potrzeb jednostki. Należy jednak także pamiętać o jego negatywnych aspektach, tj. na przykład o możliwości niewłaściwego przewidywania, które stanie się podstawą do odmowy danej osobie dostępu do jakiegoś produktu lub usługi, a w efekcie do dyskryminacji tej osoby.

Dlatego w RODO został przewidziany mechanizm obrony przed profilowaniem dla osób, które mu podlegają. Wprowadzony został generalny zakaz podejmowania wobec osoby takiej decyzji, która opierałaby się wyłącznie na zautomatyzowanym przetwarzaniu i wywoływała wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływała. Skutki prawne w tym kontekście oznaczają oddziaływanie na czyjeś prawa, a podobny wpływ można przypisać takim decyzjom, które będą znacząco wpływać na okoliczności, zachowania lub wybory danej osoby. Przykładem takich działań mogą być praktyki e-rekrutacyjne podejmowane bez interwencji człowieka lub automatyczna odmowa dotycząca wniosku kredytowego złożonego online.

Ten generalny zakaz został złagodzony poprzez wprowadzenie pewnych wyjątków – zgodnie z RODO wyłącznie automatyczne podejmowanie decyzji (w tym profilowanie) jest dopuszczalne m.in. wtedy, gdy jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, oraz administratorem (np. w przypadku produktów bankowych, ubezpieczeniowych) lub gdy opiera się na wyraźnej zgodzie osoby, której dane dotyczą. Zgoda ta musi być więc dobrowolna, jednoznaczna i wyrażona w formie oświadczenia lub wyraźnego działania osoby, której dane dotyczą. Nawet jednak wówczas, gdy zachodzą wyżej przywołane wyjątki, podmiot dokonujący profilowania musi zapewnić osobie, której dane dotyczą, możliwość uzyskania interwencji ludzkiej ze swojej strony, realizację prawa do wyrażenia własnego stanowiska oraz realizację prawa do zakwestionowania decyzji podjętej automatycznie. Osoba, której dane dotyczą, musi mieć dostęp do łatwej drogi pozwalającej jej na realizację wyżej przywołanych praw.

W przypadku profilowania na podmiocie przetwarzającym dane spoczywa dodatkowy obowiązek informacyjny, tj. klauzula informacyjna takiego podmiotu, zgodnie z RODO, powinna być rozbudowana jeszcze bardziej niż zwykle. Powinny się w niej znaleźć wszelkie informacje o tym, że podmiot ten na podstawie zebranych danych podejmuje automatycznie decyzje, w tym profiluje dane, a także informacje o tym, jakie są zasady podejmowania tych decyzji oraz znaczenie i przewidywane konsekwencje tych działań dla osoby, której dane dotyczą. W tym zakresie istotna jest kwestia, jak szczegółowo opisać w klauzuli zasady podejmowania decyzji. Zgodnie z rekomendacjami należy wskazać tylko istotne informacje o tych zasadach, a osoby, których dane dotyczą, powinny móc się zapoznać z kryteriami i logiką ich podejmowania, przy czym administrator nie ma obowiązku kompleksowego tłumaczenia algorytmów użytych w ramach tych procesów decyzyjnych.

Dodatkową instytucją wprowadzoną w ramach profilowania w RODO jest prawo osoby do wyrażenia sprzeciwu wobec takiego zautomatyzowanego przetwarzania jej danych. Sprzeciw może być wniesiony w dowolnym momencie z przyczyn związanych ze szczególną sytuacją tej osoby. W momencie gdy sprzeciw zostanie wniesiony, podmiot przetwarzający nie może w dalszym ciągu przetwarzać danych osobowych tej osoby w dotychczasowy sposób, chyba że wykaże istnienie innych ważnych, uzasadnionych prawnie podstaw do dalszego przetwarzania danych. Ten wyjątek jednak nie dotyczy profilowania na cele marketingu bezpośredniego – w takiej sytuacji prawo sprzeciwu osoby, której dane dotyczą, jest bezwarunkowe i jeśli osoba zgłosi sprzeciw, podmiot przetwarzający te dane nie będzie mógł ich już dalej przetwarzać w tym celu ani w ten sposób.

W praktyce obostrzenia dotyczące profilowania spowodują nałożenie dodatkowych obowiązków na podmioty przetwarzające dane, a wśród nich konieczność opracowania nowych procedur związanych ze zgłoszeniem sprzeciwu i realizacją praw osoby, której dane dotyczą (żądanie udziału czynnika ludzkiego, wyrażenia stanowiska, zakwestionowania decyzji podjętej automatycznie), konieczność poszerzenia obowiązku informacyjnego (w tym podjęcie decyzji, jak szczegółowe informacje na temat metod przetwarzania podać), konieczność uzyskania zgody od osoby, której dane dotyczą, jeśli administrator nie ma innych podstaw do takiego przetwarzania danych tej osoby, oraz bezwarunkowa konieczność zaprzestania profilowania, jeżeli zostanie zgłoszony sprzeciw dotyczący działań marketingowych.

Uwzględnianie ochrony danych w fazie projektowania, domyślna ochrona danych

RODO wprowadza do porządku prawnego związanego z ochroną danych osobowych dwie nowe zasady, tj. *privacy by design* (uwzględnienie ochrony danych w fazie projektowania) i *privacy by default* (domyślna ochrona danych).

Zasada *privacy by design* jest kierowana przede wszystkim do twórców aplikacji, usług i systemów, które opierają się na przetwarzaniu danych osobowych (systemy zarządzania danymi typu CRM, CMS, ERP) lub przetwarzają dane w celu realizacji swoich zadań (aplikacja mobilna sklepu internetowego). Zasada ta powinna znaleźć odzwierciedlenie w warstwie rozwiązań zarówno technicznych (to jak usługa, system są skonstruowane), jak i organizacyjnych (jakie założenia leżały u podstaw tworzenia systemu lub usługi). Wdrożenie ochrony danych już na etapie projektowania i przemyślenie wszystkich aspektów ochrony danych przed rozpoczęciem ich przetwarzania pozwalają na skuteczną i ciągłą ochronę tych danych przez cały cykl ich przetwarzania.

Zasada *privacy by default* także jest kierowana przede wszystkim do twórców rozwiązań informatycznych. Zakłada ona, że wszelkie konfiguracje ustawień prywatności w danym systemie lub aplikacji czy serwisie internetowym są dokonywane przez podmiot, którego dane są przetwarzane. Dane osoby, która korzysta z usługi udostępnionej za pośrednictwem jakiegoś systemu, aplikacji lub serwisu internetowego, powinny być od samego początku chronione w maksymalnym stopniu. Tylko świadoma decyzja osoby, która wykona stosowne zmiany w udostępnionym jej panelu administracyjnym, powinna pozwalać na zmniejszenie stopnia bezpieczeństwa ochrony danych poprzez ich udostępnianie w różnym wybranym przez tę osobę zakresie. Wprowadzenie tej zasady do RODO wynika z doświadczeń związanych z aktywnością użytkowników portali społecznościowych.

Podejście oparte na ryzyku – stałe monitorowanie zagrożeń

RODO zakłada także podejście oparte na ryzyku (*risk based approach*). W ramach tego podejścia wymaga od podmiotu przetwarzającego proaktywnego oraz zaradczego podejścia do zagadnienia ochrony danych osobowych. Podmiot przetwarzający dane osobowe ma tak dobrać środki bezpieczeństwa, aby były one najlepsze dla ochrony danych, biorąc pod uwagę poziom wystąpienia ryzyka naruszenia bezpieczeństwa, stan wiedzy technicznej oraz możliwości (finansowe, organizacyjne itp.) administratora.

Przy określaniu środków bezpieczeństwa, które będą wdrażane w zakresie ochrony danych osobowych w organizacji administratora lub podmiotu przetwarzającego, należy więc brać pod uwagę charakter, zakres, kontekst i cel dokonywanego przetwarzania danych oraz prawdopodobieństwo i wagę ewentualnego zagrożenia dla bezpieczeństwa danych.

By wykazać organowi nadzorczemu, w przypadku ewentualnej kontroli, że ta operacja została przeprowadzona przed rozpoczęciem przetwarzania danych i wprowadzeniem

stosownych środków bezpieczeństwa, dobrze zadbać o to, by została ona opisana w dokumencie, który będzie można udostępnić do wglądu w czasie kontroli.

Podejście oparte na ryzyku powinno być stosowane przez cały okres przetwarzania danych, tj. podjęte przed zebraniem danych ustalenia powinny być przez administratora aktualizowane, a w razie potrzeby (jeśli wystąpią nowe okoliczności dotyczące ryzyka związane z przetwarzaniem tych danych) – zmieniane.

Raportowanie naruszeń – organ nadzorczy i osoba, której dane dotyczą

Istotną nowością wprowadzaną przez RODO, która wiąże się z szeroko zakrojonymi regulacjami co do bezpieczeństwa przetwarzania danych osobowych, jest obowiązek zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (tj. – według projektowanej nowej polskiej ustawy o ochronie danych osobowych, która uzupełnia luki wskazane w RODO – Prezesowi Urzędu Ochrony Danych Osobowych, PUODO) lub osobie, której dotyczą dane.

Obowiązek zgłaszania naruszenia do PUODO spoczywa zarówno na administratorze, jak i na podmiocie przetwarzającym. Niezależnie od informowania PUODO podmiot przetwarzający powinien poinformować o tym naruszeniu także administratora, jeśli naruszenie dotyczy danych powierzonych mu przez tego administratora.
W przypadku gdy dojdzie do naruszenia bezpieczeństwa danych (incydent bezpieczeństwa, wyciek danych itp.) odpowiedzialny podmiot (administrator lub podmiot przetwarzający) nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia informuje o nim organ nadzorczy.

Zgłoszenie kierowane do PUODO powinno:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dotyczą dane, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane do kontaktu Inspektora Ochrony Danych lub wskazywać inny punkt do kontaktu, w którym można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać zastosowane lub proponowane przez administratora środki, które mogą przeciwdziałać naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki minimalizujące jego ewentualne negatywne skutki.

Zgłoszenia nie trzeba dokonywać, jeśli jest mało prawdopodobne, że incydent będzie skutkować ryzykiem naruszenia praw lub wolności osób fizycznych.
W przypadku opóźnienia w przekazaniu informacji do PUODO należy dołączyć do zgłoszenia wyjaśnienie przyczyn zaistniałego opóźnienia.

Poza obowiązkiem zgłaszania administrator jest zobowiązany prowadzić dokumentację wszelkich naruszeń bezpieczeństwa danych. W tej dokumentacji powinien podać okoliczności naruszenia, opisać jego skutki oraz podjęte działania zaradcze.

W przypadku gdy naruszenie ochrony danych – w ocenie administratora lub podmiotu przetwarzającego – może powodować wysokie ryzyko naruszenia praw lub wolności osób, niezależnie od powiadomienia PUODO administrator lub podmiot przetwarzający powinien zawiadomić o naruszeniu także osobę, której dane dotyczą. Powinno to nastąpić bez zbędnej zwłoki (a więc najlepiej zaraz po stwierdzeniu naruszenia, chyba że istnieją jakieś istotne okoliczności uzasadniające opóźnienie wysłania takiej informacji do osób, których dane dotyczą), jasnym i prostym językiem. Powinno wyjaśniać osobie, której dane dotyczą, charakter naruszenia, możliwe konsekwencje i podjęte działania zaradcze oraz wskazywać kontakt do Inspektora Ochrony Danych (lub innego punktu do kontaktu), który będzie mógł udzielić zainteresowanym dodatkowych informacji.

Zawiadomienie osoby, której dane dotyczą, nie zawsze jest wymagane. Obowiązek przesłania informacji nie musi zostać spełniony, jeśli:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony, a środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie; w szczególności chodzi o środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dotyczą dane;

c) jego spełnienie wymagałoby niewspółmiernie dużego wysiłku. W takim przypadku powinien zostać wydany publiczny komunikat lub podjęty inny podobny środek. Osoby, których dane dotyczą, mogą także zostać poinformowane w inny sposób – ważne, by był on równie skuteczny.

Instytucja raportowania naruszeń nakłada na administratorów i podmioty przetwarzające nowe obowiązki dotyczące wprowadzenia stosownych procedur po pierwsze wysyłania zawiadomień do organu nadzoru oraz osób, których dane dotyczą, a po drugie dokonywania oceny, na ile dane naruszenie „nadaje się" do tego, aby przesyłać o nim zawiadomienie – czyli m.in. określenia, czy jest prawdopodobne, że naruszenie będzie skutkować ryzykiem naruszenia praw lub wolności osób fizycznych (i w jakim stopniu). Ponadto konieczne będzie zawarcie stosownych zapisów w umowach powierzenia przetwarzania danych z podmiotami przetwarzającymi oraz w umowach z własnymi pracownikami i współpracownikami. Zapisy te będą dotyczyć zobowiązań tych podmiotów w zakresie raportowania naruszeń.

Biorąc pod uwagę konieczność realizacji obowiązku raportowania w ciągu 72 godzin (organ nadzoru) lub bez zbędnej zwłoki (osoba, której dane dotyczą), system informowania o naruszeniu wewnątrz organizacji oraz pozyskiwania informacji od podmiotu przetwarzającego musi być zorganizowany tak, aby był niezwykle skuteczny i szybki. Jak zwykle w przypadku regulacji RODO niedopełnienie obowiązków związanych z raportowaniem jest obwarowane wysokimi karami.

RODO a administracyjne **kary pieniężne**

Wraz z wejściem w życie RODO przedsiębiorcy powinni się liczyć ze wzmożonymi kontrolami ze strony inspektorów organu nadzorczego. Będą oni weryfikować, w jakim stopniu przedsiębiorca wdrożył nowe przepisy. Za naruszenie przepisów grożą wysokie kary pieniężne.

Karze pieniężnej do wysokości 10 mln euro,a w przypadku przedsiębiorstwa w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa) podlega m.in.:

- administrator i podmiot przetwarzający w przypadku naruszenia m.in. obowiązków otrzymania zgody przez dziecko na przetwarzanie danych osobowych, naruszenia zasad ochrony danych osobowych w fazie projektowania;
- podmiot certyfikujący – w przypadku naruszenia przepisów dotyczących certyfikacji.

Administracyjnej karze pieniężnej w maksymalnej kwocie 20 mln euro, a w przypadku przedsiębiorstwa w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa) podlega:

- naruszenie przepisów podstawowych zasad przetwarzania, w tym warunków zgody;
- naruszenie praw osób, których dane dotyczą, np. prawa do przenoszenia danych, prawa do bycia zapomnianym, prawa do informacji czy prawa dostępu;
- przekazywanie danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej;
- naruszenie wszelkich obowiązków wynikających z prawa państwa członkowskiego;
- nieprzestrzeganie nakazu tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych, orzeczonego przez organ nadzorczy.

Jak widać, górna granica kar ustawiona jest bardzo wysoko. Nie wydaje się jednak, aby kary, zwłaszcza na początku obowiązywania RODO, osiągały ten pułap.

Według danych statystycznych przedstawionych przez GIODO w 2016 roku przeprowadzono 192 kontrole, a w 2017 roku – 199. Z raportu GIODO wynika, że w 2016 roku tylko 1% badanych systemów informatycznych nie wypełniał obowiązku posiadania dokumentacji przetwarzania danych osobowych. Badanie systemów informatycznych w latach 2013–2016 pod kątem realizacji wymogów technicznych i organizacyjnych wykazały, że niemalże wszystkie obowiązki były wypełnione ze stuprocentową skutecznością.

LABORATORIUM EE

Materiał dostarczony dzięki uprzejmości Laboratorium EE

Jak przeprowadzić **audyt** i zaprojektować **wewnętrzne procesy i procedury**

T

Analiza systemów IT, ocena prawidłowości przetwarzania danych osobowych w systemach IT i rekomendacje

RODO wymaga od administratorów i podmiotów przetwarzających dane osobowe, żeby wdrożyli – każdy z nich we własnym zakresie – odpowiednie środki techniczne i organizacyjne, by zagwarantować bezpieczeństwo praw i wolności osób fizycznych, które mogłyby zostać zagrożone przy okazji przetwarzania tych danych osobowych.

Stosowane środki powinny być dostosowane do prawdopodobieństwa wystąpienia i wagi potencjalnych zagrożeń. Oprócz tego podmiot zobowiązany do zabezpieczenia procesów przetwarzania powinien wziąć pod uwagę takie czynniki, jak:

a) stan wiedzy technicznej,
b) koszt wdrażania,
c) charakter, zakres, kontekst i cele przetwarzania.

Przepisy RODO wskazują, że w stosownym przypadku podmiot zobowiązany powinien zapewnić:

a) pseudonimizację i szyfrowanie danych osobowych,
b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wynikające z przypadkowego lub niezgodnego z prawem:

a) zniszczenia,
b) utraty,
c) modyfikacji,
d) nieuprawnionego ujawnienia lub
e) nieuprawnionego dostępu do przetwarzanych danych osobowych.

Wywiązywanie się z omawianych obowiązków można wykazać m.in. poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO.

Zobowiązane podmioty muszą podejmować działania, by zagwarantować, że każda osoba fizyczna działająca z ich upoważnienia, która ma dostęp do danych osobowych, przetwarza je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii Europejskiej lub prawo państwa członkowskiego.

P

Ocena zgodności z RODO przetwarzania danych w systemach komputerowych wymaga spojrzenia na te systemy z kilku perspektyw.

Przygotuj tabelę (najlepiej w arkuszu kalkulacyjnym – będzie Ci łatwiej pracować na zebranych danych), do której wpiszesz zgromadzone informacje. Na jej podstawie możesz później stworzyć rejestr czynności przetwarzania (administrator) albo rejestr kategorii czynności przetwarzania (podmiot przetwarzający).

Obszary przetwarzania
W pierwszej kolejności należy zidentyfikować używane przez Ciebie systemy, w których przetwarzane są dane osobowe, oraz sprawdzić, jakie (oraz czyje) są to dane.

Warto spojrzeć na programy pocztowe, w których przechowujesz kontakty, aplikacje służące do wysyłania newslettera do klientów, systemy księgowe, kadrowe, CRM (*customer relationship manager*), ERP (*enterprise resource planning*), dyski wirtualne, narzędzia do współpracy w chmurze itp. Również same urządzenia, na których przechowujesz dane – komputery, laptopy, tablety, smartfony, dyski przenośne, pendrive'y – wymagają przeanalizowania pod tym kątem.

Zakresy przetwarzania
Kiedy zidentyfikujesz, gdzie przetwarzasz dane, sprawdź, jakie to są dane, posiłkując się definicją danych osobowych z RODO. Zwróć uwagę, do kogo należą te dane – Twoich pracowników, klientów, przedstawicieli kontrahentów, uczestników organizowanej konferencji czy adresatów newslettera.

P

Podstawy przetwarzania
RODO zakazuje przetwarzania danych bez podstawy prawnej. Organ nadzorczy będzie mógł Cię za to ukarać karą finansową. Żeby tego uniknąć, musisz się zastanowić nad tym, jak jesteś w stanie uzasadnić przetwarzanie danych osobowych w poszczególnych, zidentyfikowanych przez Ciebie bazach danych. Podstaw przetwarzania jest raptem siedem, więc zadanie nie powinno być bardzo trudne. Jeśli znajdziesz dane, których przetwarzania nie potrafisz uzasadnić, musisz je usunąć.

Zobacz: RODO a administracyjnea kary pieniężne
Zobacz: Fundamentalne zasady przetwarzania danych

Cele i okresy przetwarzania
Przeglądając wpisy w bazach danych, z pewnością znajdziesz dane osobowe sprzed wielu lat. Mogą to być na przykład CV kandydatów do pracy, którzy zostali odrzuceni, przechowywane na wszelki wypadek. Bardzo możliwe, że będzie trzeba się z nimi rozstać. RODO nakazuje ograniczyć okres przechowywania danych do niezbędnego minimum, uzasadnionego celem przetwarzania. Innymi słowy, jeśli dane klienta są Ci potrzebne, by wykonać zawartą z nim umowę – możesz przechowywać jego dane do czasu wykonania tej umowy i ewentualnie przez okres przedawnienia roszczeń z tytułu tej umowy (zwykle 2/3/10 lat, w zależności od umowy). Jeśli podstawą przetwarzania jest zgoda użytkownika, dopuszczalny okres będzie wynikał z zakresu zgody udzielonej na jeden lub kilka konkretnych celów przetwarzania. W przypadku przesłanki prawnie uzasadnionego interesu administratora lub strony trzeciej musisz się zastanowić, jaki okres przetwarzania obejmuje Twój prawnie uzasadniony interes – i przekonać do tego stanowiska organ nadzorczy.

Minimalizacja danych
Czy wszystkie dane, które przetwarzasz, są Ci potrzebne do osiągnięcia celu, w którym je zbierasz? RODO pozwala na zbieranie danych adekwatnych i niezbędnych do celu przetwarzania. Jeśli np. by zapisać się do Twojego newslettera, użytkownik serwisu musiał podać numer telefonu, adres lub wykształcenie – dane obiektywnie niepotrzebne do realizacji wysyłki – przetwarzanie tych danych jest niezgodne z przepisami i takie informacje powinny zostać usunięte.

Bezpieczeństwo przetwarzania
RODO mówi o środkach technicznych i organizacyjnych, które mają zapewnić zachowanie praw i wolności osób fizycznych, związane z przetwarzaniem przez Ciebie ich danych osobowych. O co chodzi?

Środki techniczne to fizyczne lub elektroniczne zabezpieczenia, które mają minimalizować ryzyko naruszenia bezpieczeństwa danych osobowych.
W przypadku przetwarzania danych w formie elektronicznej chodzi o wiele rozwiązań, takich jak:

a) oprogramowanie antywirusowe;
b) *firewall*;
c) szyfrowanie plików zawierających dane osobowe (w czasie przechowywania na dysku, a także w czasie przesyłania ich przez internet do odbiorców);
d) kontrola dostępu do urządzeń, za pośrednictwem których dochodzi do przetwarzania danych osobowych (loginy i hasła, automatyczne blokowanie ekranu po możliwie krótkim okresie bezczynności itp.);
e) kontrola dostępu do pomieszczeń, w których znajdują się te urządzenia (karty magnetyczne, zamki i klucze, kraty okienne, żaluzje antywłamaniowe itp.);
f) odpowiednia architektura sieci komputerowych, w których przesyłane są dane osobowe (wyodrębnienie obszarów z różnymi poziomami dostępu i zakresami przetwarzanych danych);
g) monitoring wizyjny pomieszczeń, w których przetwarzane są dane osobowe.

Ryzyka, które RODO każe brać pod uwagę, to nie tylko wyciek danych, ale też m.in. ich utrata lub zniszczenie, dlatego należy wziąć pod uwagę również:

a) regularne tworzenie kopii zapasowych danych osobowych;
b) zapewnienie alternatywnego zasilania serwerów, na których przechowywane są dane osobowe;
c) zapewnienie w serwerowni środków bezpieczeństwa pożarowego.

Środki organizacyjne to nic innego, jak procedury i polityki, które mają zminimalizować ryzyko naruszenia bezpieczeństwa danych osobowych w Twojej organizacji. Postanowienia tego rodzaju mogą się znajdować w jednym lub kilku dokumentach – polityce prywatności, polityce ochrony danych osobowych, regulaminie pracy, w treści umów z pracownikami lub w innego rodzaju regulaminie.

Polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, wdrożone w okresie obowiązywania UODO*, zdecydowanie spełniają tę funkcję. Przejrzyj je jednak i zaktualizuj pod kątem nowych regulacji RODO.

* Ustawa o ochronie danych osobowych.

P

Polityka powinna zawierać postanowienia dotyczące bezpiecznego postępowania z danymi. Możesz w niej zawrzeć na przykład:

a) określenie zasad nadawania uprawnień do przetwarzania danych osobowych;
b) określenie zasad postępowania przy pozyskiwaniu, wykorzystywaniu, usuwaniu danych osobowych (np. kto i kiedy ma realizować obowiązek informacyjny wobec osób, których dane są pozyskiwane);
c) obowiązki określonych kategorii pracowników w zakresie ewidencjonowania i kontrolowania upoważnień do przetwarzania danych osobowych, tworzenia i korzystania z baz danych osobowych;
d) zasadę czystego biurka;
e) zasadę czystego ekranu;
f) wskazanie środków ostrożności, które należy zachować przy wynoszeniu nośników z danymi osobowymi poza teren biura (lub zakaz takiego postępowania);
g) zasady dotyczące polityki tworzenia i zmieniania haseł do komputerów, systemów operacyjnych itp.;
h) zasady dotyczące korzystania z prywatnych urządzeń pracowników do celów przetwarzania danych osobowych, których administratorem lub podmiotem przetwarzającym jest Twoja organizacja (lub zakaz takiego postępowania);
i) procedury realizacji uprawnień osób, których dotyczą dane osobowe;
j) procedury raportowania naruszeń bezpieczeństwa danych osobowych do organu nadzorczego/osób, których dotyczą dane.

Zobacz: Nowe (i stare) uprawnienia osób, których dane dotyczą
Zobacz: Nowe regulacje wprowadzone przez RODO

Dokumenty powinny być zrozumiałe dla ich adresatów (Twojego personelu), a zawarte w nich zasady – rzeczywiście stosowane. Inspektorowi przeprowadzającemu kontrolę w Twojej organizacji nie wystarczy sam fakt stworzenia określonego, „martwego" dokumentu. Warto przewidzieć mechanizm cyklicznej weryfikacji przestrzegania i ewentualne konsekwencje za naruszenie ustanowionych zasad. Również same zasady powinny podlegać regularnym przeglądom i, w razie potrzeby, aktualizacjom.

Zwróć uwagę, że potencjalne zagrożenia powinny być oceniane z perspektywy osób fizycznych, których dotyczą przetwarzane dane osobowe, a nie z perspektywy podmiotu zobowiązanego do wdrożenia środków bezpieczeństwa (Twojej organizacji). To bardzo istotne, bo ta optyka (postawienie się w sytuacji osoby, której dotyczą dane osobowe) powinna Ci towarzyszyć przez cały proces audytu i dostosowywania Twojej organizacji do przepisów RODO.

Funkcjonalności

Wiesz już, jakie uprawnienia będą przysługiwały osobom, których dotyczą dane osobowe. Na tym etapie audytu musisz sprawdzić, czy jesteś w stanie je zrealizować przy użyciu swoich narzędzi informatycznych. Sprawdź, czy używane przez Ciebie systemy mają funkcje, które umożliwią Ci eksport danych do formatu interoperacyjnego, ograniczenie ich przetwarzania lub ich szybkie usunięcie. W razie wątpliwości skontaktuj się z opiekunem produktu, którego dane powinny się znajdować w umowie licencyjnej, albo po prostu zadzwoń na infolinię producenta. Możliwe, że posiadana przez Ciebie wersja oprogramowania nie oferuje odpowiednich funkcji, ale możesz ją zaktualizować do wersji zgodnej z RODO.

Zobacz: Nowe (i stare) uprawnienia osób, których dane dotyczą

Analizując powyższe aspekty i decydując się na określone działania dostosowawcze, pamiętaj o tym, że to do Ciebie należy ocena adekwatności stosowanych środków do Twojej sytuacji. RODO każe brać pod uwagę charakter, zakres, kontekst i cele przetwarzania, ale także koszty wdrażania. Nie martw się, że musisz poświęcić 50% budżetu organizacji na zakup nowoczesnego sprzętu i oprogramowania. Działaj w skali odpowiedniej do Twojej organizacji i zagrożeń dla operacji przetwarzania danych, które prowadzisz.

P

Analiza papierowych zbiorów danych osobowych i ocena prawidłowości przetwarzania danych osobowych w formie papierowej oraz rekomendacje

Do papierowych baz danych osobowych można odnieść także uwagi na temat przetwarzania danych w systemach komputerowych, z uwzględnieniem specyfiki papierowej formy przetwarzania danych.

Zobacz: Analiza systemów IT, ocena prawidłowości przetwarzania danych osobowych w systemach IT i rekomendacje

Obszary przetwarzania

Sprawdź, gdzie w Twojej organizacji przechowywane są dokumenty zawierające dane osobowe. Jeśli dbasz o bezpieczeństwo danych, będą w większości zgromadzone w bezpiecznym archiwum. Należy się jednak spodziewać, że jakieś teczki lub segregatory znajdują się w różnych pokojach, przy biurkach pracowników, przy recepcji, w miejscach, gdzie przydają się w codziennej pracy. Jeśli z perspektywy funkcjonowania organizacji nie jest możliwe skupienie ich wszystkich w jednym miejscu, opisz te miejsca w osobnej tabeli – **wykazie pomieszczeń, w których przetwarzane są dane osobowe**. Będzie też trzeba odpowiednio zabezpieczyć te pomieszczenia.

Bezpieczeństwo przetwarzania

Identyfikacja zagrożeń dla zbiorów papierowych będzie łatwiejsza dla przeciętnej osoby niż przewidzenie ryzyk, które dotykają zbiorów elektronicznych. Dlatego w przypadku zabezpieczenia dokumentów fizycznych najlepszym doradcą będzie zdrowy rozsądek.

Podobnie jak przy zbiorach elektronicznych, również tutaj znajdą zastosowanie środki techniczne i organizacyjne.

Przykładowe środki techniczne:

a) kontrola dostępu do dokumentów zawierających dane osobowe (sejfy, szafy pancerne, szafy meblowe zamykane na klucz; to, kto ma mieć dostęp do klucza, powinna określać odpowiednia polityka);
b) kontrola dostępu do pomieszczeń, w których znajdują się dane osobowe (karty magnetyczne, zamki i klucze, kraty okienne, żaluzje antywłamaniowe itp.);
c) zapewnienie w pomieszczeniach, w których przetwarzane są dane osobowe, środków bezpieczeństwa pożarowego;
d) monitoring wizyjny pomieszczeń, w których przetwarzane są dane osobowe.

Przykładowe środki organizacyjne (zawartość polityki):

a) wspomniana już polityka udostępniania kluczy (wraz z ewidencją ich wydań i zwrotów);
b) zasada czystego biurka;
c) zasady dotyczące wynoszenia dokumentów papierowych zawierających dane osobowe poza teren biura;
d) ewidencja pomieszczeń, w których przetwarzane są dane osobowe;
e) zasady korzystania z pomieszczeń, w których przetwarzane są dane osobowe, w tym ich zamykania na okres poza godzinami pracy, dostępu do nich osób postronnych (klientów, personelu sprzątającego, konserwatorów budynku) itp.

T

Analiza dokumentów kadrowych i ewentualna modyfikacja

Przepisy RODO co do przetwarzania danych pracowników będą uzupełnione przepisami znowelizowanego Kodeksu pracy. Modyfikacje aktualnego brzmienia kodeksu przewiduje projekt ustawy o roboczym tytule „o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679". Jego najnowsza (na dzień publikacji niniejszego poradnika) wersja została przygotowana przez Radę Ministrów 28 marca 2018 roku.

Aktualny projekt przewiduje m.in. następujące przepisy (nowe lub w zmodyfikowanym brzmieniu).

”

Art. 22^1

§1. Pracodawca żąda od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących:
1) imię (imiona) i nazwisko;
2) datę urodzenia;
3) dane kontaktowe wskazane przez taką osobę;
4) wykształcenie;
5) przebieg dotychczasowego zatrudnienia.

§2. Pracodawca żąda od pracownika podania dodatkowo danych osobowych obejmujących:
1) adres zamieszkania;
2) numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość;
3) inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy.

§3. Pracodawca żąda podania innych danych osobowych niż określone w §1 i 2, gdy jest to niezbędne do wypełniania obowiązku pracodawcy nałożonego przepisem prawa.

§4. Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Pracodawca może żądać udokumentowania danych osobowych osób, o których mowa w §1 i 2, w zakresie niezbędnym do ich potwierdzenia.

Art. 22^2

§1. Przetwarzanie przez pracodawcę innych danych osobowych niż wymienione w art. 221 §1 i 2 jest dopuszczalne za zgodą osoby ubiegającej się o zatrudnienie lub pracownika i tylko wtedy, gdy jest to dla nich korzystne.

§2. Brak zgody, o której mowa w §1 lub jej wycofanie, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę.

§3. Przetwarzanie, o którym mowa w §1, dotyczy danych osobowych udostępnianych przez osobę ubiegającą się o zatrudnienie lub pracownika na wniosek pracodawcy lub danych osobowych przekazanych pracodawcy z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika.

Art. 22^3

§1. Przetwarzanie danych osobowych, o których mowa w art. 9 ust. 1 i art. 10 [RODO – przyp. red.], jest dopuszczalne tylko wtedy, gdy jest to niezbędne do wypełniania obowiązku pracodawcy nałożonego przepisem prawa.

§2. Przetwarzanie danych biometrycznych pracownika jest dopuszczalne także wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę lub dostępu do pomieszczeń wymagających szczególnej ochrony.

Art. 22^4

§1. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).

§2. Monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek, palarni lub pomieszczeń udostępnianych zakładowej organizacji związkowej, chyba, że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego § 1 i nie naruszy to godności oraz innych dóbr osobistych pracownika, a także zasady wolności i niezależności związków zawodowych, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób.

§3. Nagrania obrazu pracodawca przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres nieprzekraczający 3 miesięcy.

§4. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu lub pracodawca powziął wiadomość,

T

iż mogą one stanowić dowód w postępowaniu, termin określony w §3 ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

§5. Po upływie okresów, o których mowa w §3 lub 4, uzyskane w wyniku monitoringu nagrania obrazu, podlegają zniszczeniu.

§6. Cele, zakres oraz sposób zastosowania monitoringu ustala się w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy.

§7. Pracodawca informuje pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem.

§8. Pracodawca przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje, o których mowa w § 6.

§9. W przypadku wprowadzenia monitoringu pracodawca oznacza pomieszczenia monitorowane w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem.

§10. Przepis §9 nie narusza art. 12 i 13 [RODO – przyp. red.].

Art. 22^5

§1. Jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, pracodawca może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej).

§2. Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.

§3. Przepis art. 224 §6-10 stosuje się odpowiednio.

§4. Przepisy §1-3 stosuje się odpowiednio do innych form monitoringu, jeśli ich zastosowanie jest konieczne do realizacji celów, określonych w §1.

P

Przetwarzanie danych pracowników w kontekście RODO powinno zostać przeanalizowane w taki sam sposób, jak przetwarzanie innych kategorii danych. Specyfika tej kategorii sprowadza się do tego, że – poza RODO – mają tu dodatkowo zastosowanie regulacje prawnopracownicze.

Zakres przetwarzania

Projektowany Kodeks pracy zawiera ograniczony katalog danych, których może żądać pracodawca od kandydata do pracy lub pracownika. W tym wypadku zasada minimalizacji danych jest więc dodatkowo zaostrzona.

Okres przetwarzania

W kontekście przetwarzania danych kandydatów do pracy trzeba pamiętać w szczególności o zasadzie ograniczenia przechowywania. Niedopuszczalne jest przechowywanie otrzymanych CV i listów motywacyjnych przez czas nieograniczony. Po zakończeniu procesu rekrutacji należy usunąć zawarte w nich dane osobowe, chyba że masz zgodę na przetwarzanie danych na potrzeby kolejnych rekrutacji.

Obecnie ustawa określa okres przechowywania danych pracowniczych na 50 lat. Od 1 stycznia 2019 roku czas ten skróci się do 10 lat na mocy Ustawy z dnia 10 stycznia 2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją (Dz.U. 2018 poz. 357). Po upływie tego okresu dane powinny zostać usunięte lub zanonimizowane.

Podstawa przetwarzania

Podstawą przetwarzania danych osobowych pracownika będą co do zasady przepisy prawa pracy. Co do zasady, bo określone cele przetwarzania, wykraczające poza standardowy stosunek pracy (dodatkowe świadczenia i korzyści dla pracownika, opcjonalne uczestnictwo w określonych programach, wydarzeniach itp.) nie będą objęte tą podstawą prawną. W tej sytuacji trzeba zidentyfikować inną podstawę przetwarzania i ewentualnie podjąć dodatkowe czynności (jeśli podstawą miałaby być zgoda pracownika – uzyskać stosowną zgodę w formie pozwalającej na potwierdzenie jej udzielenia w przypadku kontroli organu nadzorczego).

Pamiętaj również o tym, że wobec kandydatów do pracy i pracowników należy zrealizować obowiązek informacyjny określony w art. 13 lub 14 RODO (w zależności od tego, skąd pozyskujesz ich dane – bezpośrednio od nich czy z innych źródeł, np. z portalu rekrutacyjnego).

T

Analiza przekazywania danych osobowych podmiotom trzecim; opracowanie nowego wzoru umowy powierzenia przetwarzania danych osobowych

Art. 28 RODO

Jeżeli przetwarzanie danych osobowych ma być dokonywane w imieniu administratora, wolno mu korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Podmiotowi przetwarzającemu nie wolno korzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający powinien informować administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

Przetwarzanie przez podmiot przetwarzający może się odbywać wyłącznie na podstawie umowy o powierzeniu przetwarzania danych osobowych lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego, wiążą podmiot przetwarzający i administratora i określają:

a) przedmiot przetwarzania,
b) czas trwania przetwarzania,
c) charakter przetwarzania,
d) cel przetwarzania,
e) rodzaj danych osobowych,
f) kategorie osób, których dane dotyczą,
g) obowiązki i prawa administratora.

Umowa o powierzeniu przetwarzania danych osobowych (lub inny instrument prawny) musi mieć formę pisemną (w tym formę elektroniczną) i wskazywać, że podmiot przetwarzający:

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmuje wszelkie środki wymagane na mocy art. 32 RODO (bezpieczeństwo przetwarzania);
d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 RODO;
e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;
g) po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji administratora, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania, że powyższe obowiązki zostały spełnione, oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Podmiot przetwarzający powinien niezwłocznie poinformować administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii Europejskiej lub państwa członkowskiego o ochronie danych osobowych.

Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, który podlega prawu Unii Europejskiej lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem

przetwarzającym, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

Wystarczające gwarancje, o których mowa powyżej, podmiot przetwarzający może wykazać m.in. poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 RODO, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO.

Bez uszczerbku dla indywidualnych umów między administratorem a podmiotem przetwarzającym umowa lub inny akt prawny, o których mowa powyżej, mogą się opierać w całości lub w części na standardowych klauzulach umownych, określonych przez Komisję Europejską, także gdy są one elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43 RODO.

Również krajowy organ nadzorczy może przyjąć standardowe klauzule umowne dotyczące kwestii, o których mowa powyżej, zgodnie z mechanizmem spójności, o którym mowa w art. 63 RODO.

Jeżeli podmiot przetwarzający naruszy przepisy RODO przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

P

Kwestia powierzenia przetwarzania danych osobowych często budzi wątpliwości administratorów danych. Szczególnie kłopotliwe wydaje się rozróżnienie sytuacji, w których dochodzi do powierzenia przetwarzania danych osobowych podmiotowi przetwarzającemu, od tych, w których dochodzi do udostępnienia danych innemu administratorowi.

Podstawą dokonania rozróżnienia jest dokładne zapoznanie się z definicjami administratora i podmiotu przetwarzającego. Jeśli podmiot, któremu przekazujesz dane osobowe, przetwarza je wyłącznie w Twoim imieniu i na Twoje polecenie – jest podmiotem przetwarzającym. Jeśli występuje wobec osób, których dane mu przekazujesz, we własnym imieniu, i samodzielnie decyduje o tym, co robi z tymi danymi – jest (niezależnym od Ciebie) administratorem.

Zobacz: Nowe regulacje wprowadzone przez RODO

W jakich jednak przypadkach dochodzi do powierzenia przetwarzania danych osobowych? Niektóre przypadki są dość oczywiste, inne łatwiej przeoczyć.

Przekazując dane swoich pracowników do biura rachunkowego w celu prowadzenia rozliczeń, powierzasz mu w tym zakresie dane osobowe. Biuro rachunkowe nie działa we własnym imieniu, a jedynie przygotowuje na Twoje zlecenie odpowiednie wyliczenia i dokumenty, którymi zarządzasz samodzielnie. Najczęściej dysponuje też pełnomocnictwem do działania w Twoim imieniu, co dodatkowo ujednoznacznia tę sytuację.

Podobna sytuacja będzie miała miejsce w przypadku współpracy z agencją marketingową, *call center*, zewnętrznym przedstawicielem handlowym czy firmą kurierską, którym przekazujesz dane swoich klientów.

Zwróć jednak uwagę, że w ramach działalności swojej organizacji powierzasz przetwarzanie danych osobowych również innym podmiotom.

Chodzi tu m.in. o dostawców oprogramowania, z którego korzystasz na zasadzie *software as a service*, w tym wszelkich rozwiązań chmurowych. Wprowadzając do komputera dane, które następnie przechowywane są na serwerach firmy zewnętrznej, udzielasz tym podmiotom dostępu do swoich baz danych i umawiasz się z nimi, że będą je dla Ciebie przechowywać. A przechowywanie to – jak już wiesz – jedna z form przetwarzania danych.

Co więcej, w powyższych sytuacjach – ze względu na lokalizację największej liczby serwerowni – może dojść do przekazania danych do państw trzecich (spoza Europejskiego Obszaru Gospodarczego), a zapewne również do państw, które nie gwarantują wystarczającego (zgodnie z wytycznymi RODO) poziomu ochrony danych osobowych. Taki transfer danych będzie wymagał zapewnienia odpowiednich gwarancji bezpieczeństwa danych, wymaganych przez przepisy rozporządzenia.

Innym przykładem jest korzystanie z usług firmy ochroniarskiej, która prowadzi monitoring wizyjny Twojego sklepu, biura, magazynu itp. Upoważniając tę firmę do prowadzenia monitoringu, udzielasz jej dostępu do wizerunku swoich gości (klientów, kontrahentów, współpracowników), który może stanowić daną osobową.

Zobacz: Kogo dotyczy RODO

Zdarzają się również bardziej skomplikowane sytuacje, w których role się odwracają i to Ty okazujesz się

podmiotem przetwarzającym w odniesieniu do tych samych danych, którymi zarządzasz. Może to mieć miejsce np. w sytuacji, w której zawrzesz z prywatną kliniką umowę o świadczenie usług prywatnej opieki medycznej dla swoich pracowników. Oczywiście jesteś administratorem danych swoich pracowników. Zawierając umowę z kliniką, zobowiążesz się do tego, że zbierzesz od pracowników deklaracje przystąpienia do pakietu opieki medycznej i przekażesz je klinice. W tej sytuacji będziesz działać w imieniu kliniki, a zatem Twoja firma powinna zawrzeć z nią umowę powierzenia przetwarzania danych osobowych jako podmiot przetwarzający.

Postanowienia, które powinna zawierać umowa powierzenia przetwarzania danych osobowych, dokładnie określa art. 28 RODO.

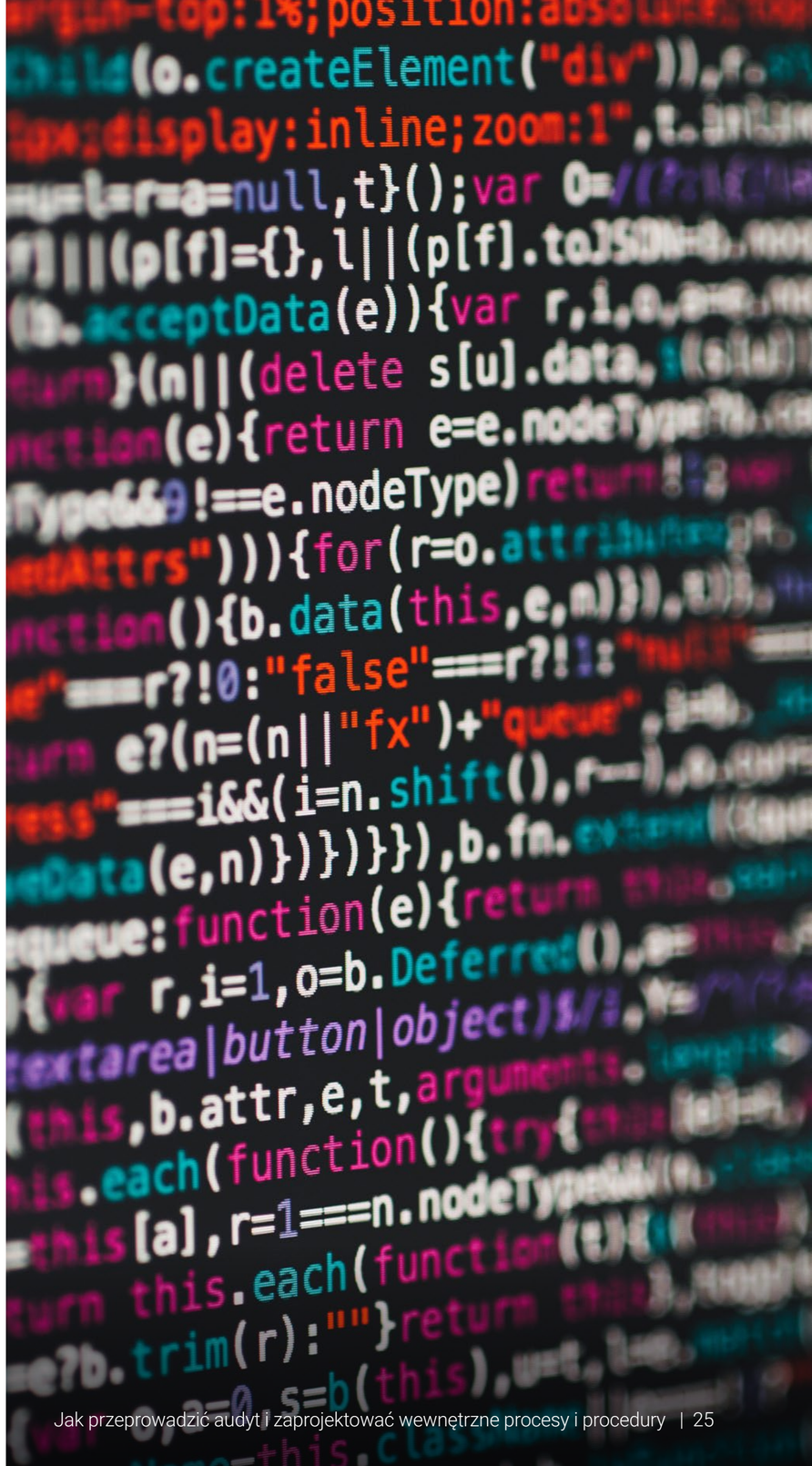
Podmiot przetwarzający powinien działać wyłącznie na Twoje wyraźne polecenie, zawarte w samej umowie lub zakomunikowane później, chyba że określonego działania wymaga od niego obowiązujące prawo. Poniesie odpowiedzialność za wszelkie operacje na danych osobowych dokonane wbrew Twojemu poleceniu lub z nim niezgodne, chyba że Twoje polecenie jest niezgodne z prawem.

Podmiot przetwarzający powinien dbać o bezpieczeństwo danych osobowych we własnym zakresie, a także wspierać Cię w wykonywaniu Twoich obowiązków. Jest też wprost zobowiązany do poinformowania Cię, jeśli uważa, że Twoje polecenie jest niezgodne z prawem.

Odpowiadasz za wybór właściwego podmiotu przetwarzającego. W szczególności musisz uzyskać dostateczną pewność, że będzie on w stanie wykonywać swoje obowiązki rzetelnie i prawidłowo oraz że daje rękojmię właściwej ochrony powierzonych mu danych osobowych.

Musisz być również w stanie wykazać, że Twoja firma dołożyła należytej staranności w tym zakresie. RODO wskazuje na możliwość legitymowania się przez podmiot przetwarzający stosownym certyfikatem lub stosowaniem określonego zatwierdzonego kodeksu postępowania, jednak zanim te pojawią się na rynku, minie trochę czasu.

Wybór renomowanego i znanego na rynku podmiotu zwiększa szanse na to, że daje on właściwe gwarancje. Oprócz tego w umowie powierzenia przetwarzania danych osobowych należy zawrzeć obowiązkowe postanowienia o możliwości audytowania podmiotu przetwarzającego. Dodatkowym atutem będzie dołączenie do umowy wykazu informacji o stosowanych przez podmiot przetwarzający środkach technicznych i organizacyjnych, służących zapewnieniu bezpieczeństwa przetwarzania danych osobowych. Nic nie stoi także na przeszkodzie, by umowa przewidywała możliwość nałożenia na podmiot przetwarzający kary umownej (za naruszenie postanowień umownych, niezależnie od odpowiedzialności odszkodowawczej podmiotu przetwarzającego wobec osób, których dotyczą dane osobowe) lub administracyjnej (w przypadku ukarania go przez organ nadzorczy).



T *teoria* + P *praktyka*

Co widać na zewnątrz – **analiza klauzul i polityk**

T

Katrzyna Szymielewicz
Co-founder i Prezes,
Fundacja Panoptykon

„I żyli długo i szczęśliwie…" – tak dzieje się tylko w komediach romantycznych. W prawdziwym życiu dobra relacja wymaga częstego zasiadania przy stole negocjacyjnym. Akceptujemy to, gdy chodzi o pracę czy rodzinę, ale przenoszenie tego modelu na wszystkie sfery życia doprowadziłoby nas do białej gorączki. Nie lubimy być na każdym kroku pytani o zdanie i zmuszani do podejmowania decyzji. W internecie wszystko powinno po prostu działać: gładko i intuicyjnie. Na tym oczekiwaniu wyrosły modele biznesowe, które nadużywają naszego zaufania: ważne informacje ukrywają pod drobną czcionką, zbierają więcej danych, niż potrzebują, przyjmują ryzykowne założenia („skoro klient nie protestuje, to pewnie się zgadza"). A kiedy się okazuje, że usługa albo urządzenie robi za naszymi plecami coś, na co byśmy się nie zgodzili, czujemy się oszukani. Gdzie leży złoty środek między poszanowaniem naszego wyboru a zapewnieniem dobrego doświadczenia użytkownikowi? RODO ma na to przepis.

Zgodnie z nowym prawem o ochronie danych osobowych administrator ma obowiązek zapytać, zanim sięgnie po dane, które nie są mu potrzebne. Ale też nie powinien zawracać nam głowy niepotrzebnymi komunikatami. RODO w żadnym razie nie wymaga zalewania nas pop-upami z nagabywaniem „czy akceptujesz…?". W praktyce takie pytanie powinno być wyjątkiem, a nie regułą. Właśnie po to administrator ma inne podstawy prawne, żeby z nich korzystać. Jeśli administrator zamierza np. przetwarzać tylko te dane, które są potrzebne do zrealizowania zawartej umowy, albo takie, których wymaga od niego obowiązujące prawo, nie musi nam zawracać głowy żadnymi pytaniami. Wystarczy, że nas o swoich zamiarach poinformuje. W innych przypadkach powinien się kierować kilkoma prostymi zasadami:

Zasada numer 1: zapytaj mnie o zdanie!

Zgodnie z artykułem 7 ust. 4 RODO wysoce niepożądane jest łączenie zgód z akceptacją warunków świadczenia usługi w sytuacji, gdy taka zgoda nie jest niezbędna do jej realizacji. Innymi słowy nie możesz, jako usługodawca, żądać od klienta zgody na przetwarzanie danych, które nie są konieczne do wykonania danej usługi (musi istnieć bezpośrednie i obiektywne powiązanie między przetwarzaniem danych i celem wykonania umowy). Niezbędne są na przykład: adres, który jest konieczny do dostarczenia towaru, czy dane karty kredytowej, potrzebne do przeprowadzenia procesu płatności. Jednak tutaj zastosowanie ma inna podstawa prawna i pozyskanie takiej zgody na warunkach opisanych w RODO nie jest konieczne.

Oczywiście dalej możesz sięgnąć po dane, których tak naprawdę nie potrzebujesz, ale które mogą Ci się przydać,

gdy taką zgodę otrzymasz. Jednak pamiętaj o tym, że nie możesz projektować procesu pozyskiwania zgód tak, aby osoba odwiedzająca Twoją stronę, sklep lub korzystająca z Twojej aplikacji musiała za jednym zamachem wyrazić zgodę na wszystko – również na to, co nie jest Ci bezwzględnie potrzebne.

Dobrze zadane pytanie o zgodę na przetwarzanie danych osobowych buduje relację: daje pytanemu poczucie kontroli, a pytającemu – wiedzę o granicach drugiej strony. I przy okazji daje Ci pewność, że taka zgoda jest w świetle RODO ważna.

To pytanie ma sens tylko wtedy, kiedy jesteś w stanie uszanować każdą odpowiedź. „Tak, możesz przetwarzać moje dane w tym celu" – świetnie, chętnie z tego skorzystam. „Nie, nie zgadzam się!" – nie ma problemu, w takim razie nie będziemy tego robić. Jeśli tak naprawdę masz inny plan i zadajesz pytanie tylko po to, aby usłyszeć „tak", to wtedy mamy do czynienia ze zgodą, która nie jest dobrowolna. I tym samym jest nieważna.

Musisz pamiętać, że dane, które ktoś Ci dobrowolnie przekazał, pozostają tak naprawdę poza Twoją kontrolą – osoba, której dane przetwarzasz, może bowiem w dowolnym momencie cofnąć swoją zgodę. Dlatego nie powinny one być podstawą Twoich działań, bo dziś je masz, ale jutro możesz je stracić.

Zasada numer 2: graj uczciwie!

Skuteczne, czyli zgodne z RODO, pozyskanie zgody na przetwarzanie danych osobowych wcale nie jest łatwe. I – powiedzmy to sobie wprost – nie ma nic wspólnego z uganianiem się za irytującym okienkiem, które zasłania treść na stronie internetowej. Chodzi o partnerski dialog, w którym szczerze przyznajesz, do czego te dane się przydadzą, a pytany ma przestrzeń, żeby się zastanowić i podjąć świadomą decyzję. Udzielona zgoda powinna być:

- **jednoznaczna**, a więc nie powinna pozostawiać wątpliwości co do tego, na co dana osoba się zgadza (np. czy na przetwarzanie dodatkowych danych w celu marketingowym, czy tylko na zawarcie umowy);
- **dobrowolna**, a więc niewymuszona negatywnymi konsekwencjami (np. pop-upem, który ostrzega, że bez „zgody" na przetwarzanie danych nie będzie można skorzystać z usługi albo serwis nie będzie działał poprawnie);
- **świadoma**, czyli oparta na wcześniej przekazanych, rzetelnych i zrozumiałych informacjach.

W żadnym wypadku nie może zostać uznane za zgodę na przetwarzanie danych milczenie osoby, której dane dotyczą, lub niepodjęcie przez nią działania.

Ale to jeszcze nie koniec! Żeby mieć pewność, że zgoda jest udzielona w jednoznaczny, dobrowolny i świadomy sposób, musisz zadbać o kilka ważnych drobiazgów:

- **wyodrębnienie zgody** (niedopuszczalne jest „spakowanie" zgody do regulaminu czy polityki prywatności, które akceptujemy, zawierając umowę);
- napisanie jej **jasnym i prostym językiem** (to warunek podjęcia decyzji w świadomy sposób);
- wyjaśnienie, **w jakim celu i przez kogo dane będą przetwarzane** (jeśli tych celów jest więcej niż jeden albo gdy w grę wchodzi przetwarzanie danych przez inny podmiot, trzeba o to zapytać osobno);
- **doświadczenie użytkownika** – prośba o udzielenie zgody nie może niepotrzebnie utrudniać korzystania z usługi, której dotyczy (wyskakujące okienka i bannery muszą odejść do lamusa!).

Zasada numer 3: nie blefuj!

Zgodę w każdej chwili można cofnąć. Nie da się na niej oprzeć stabilnego biznesu.

Powtórzmy to jeszcze raz: dane można przetwarzać w oparciu o różne podstawy prawne, nie tylko zgodę. Pozyskanie takiego oświadczenia woli wymaga dodatkowego wysiłku, a do tego w każdej chwili można je stracić. A więc nie da się na nim oprzeć stabilnego biznesu ani realnie zarobić (bo co to za zasób, który w każdej chwili może zniknąć?). Dlatego w komercyjnych relacjach warto zachować dystans i sceptycyzm wobec firm, które zbyt często pytają nas o zgodę na przetwarzanie danych. Może to działanie pozorne? Albo obliczone na określony efekt? Zgoda pozyskana w wyniku manipulacji czy dezinformacji nie tylko jest nieważna na gruncie RODO (a więc wiąże się z naruszeniem prawa i ryzykiem wysokich sankcji), ale też niszczy reputację i podważa zaufanie do administratora, który gra nieczysto.

W kwestii wycofania zgody musisz pamiętać o tym, żeby ten proces był tak samo łatwy, jak proces jej udzielenia. Nie musi on być identyczny, ale z praktyki wynika, że powinien być podobny. W tym przypadku, jeśli proces cofnięcia zgody jest dużo bardziej skomplikowany niż proces jej pozyskania, w świetle RODO sama zgoda również jest nieważna.

T

Zasada numer 4: nie wszystkie zgody idą do kosza po wprowadzeniu RODO

RODO nie jest pierwszym unijnym aktem prawnym, który wprowadza wymogi dotyczące uzyskiwania zgód. Dotychczas obowiązywała dyrektywa 95/46/WE. RODO nie jest całkowitą nowością, jednak podnosi poprzeczkę. Dlatego jako administrator danych nie musisz od nowa pozyskiwać wszystkich zgód, które już posiadasz. Musisz jednak dokonać ich przeglądu, aby mieć pewność, że zostały pozyskane zgodnie z nowymi zasadami, o których piszemy powyżej. Musisz je natomiast zebrać na nowo w sytuacji, gdy dotychczasowe zgody były domniemane i nie przechowujesz na ich temat żadnych danych (a więc nie jesteś w stanie wykazać, że je uzyskałeś/uzyskałaś).

Nowe przepisy zostawiają także inne koło ratunkowe – zgoda dostosowana do wymogów RODO jest tylko jednym z istniejących w prawie sposobów sankcjonujących przetwarzanie danych. Dlatego jeśli istnieje taka możliwość, możesz znaleźć inną podstawę prawną do przetwarzania danych pozyskanych przed 25 maja. Jednak jest to zabieg jednorazowy: po wejściu w życie RODO tego typu żonglerka będzie już zabroniona.

P

Dobrowolność zgody

Na gruncie RODO zgoda ma sens wtedy (i tylko wtedy!), kiedy administrator próbuje sięgnąć po dane, których tak naprawdę nie potrzebuje, ale z których chętnie skorzysta, jeśli mu na to pozwolimy. Nie może uzasadnić swojej ciekawości żadną inną podstawą prawną. Typowe przykłady takich sytuacji:

- zbieranie informacji o lokalizacji użytkowników aplikacji online w celach marketingowych;
- odpytywanie klientów sklepów o to, gdzie mieszkają (kod pocztowy) albo do jakiego przedziału wiekowego należą, nawet gdy nie dokonują zakupu;
- zbieranie dodatkowych informacji kontaktowych (np. numeru telefonu), jeśli ma to się przyczynić wyłącznie do usprawnienia komunikacji;
- przekazywanie danych zebranych w jednym celu (np. na potrzeby scoringu kredytowego) partnerom z grupy kapitałowej w innym celu (np. marketingowym).

Niedopuszczalne jest także łączenie zgód w „pakiety”, zawierające zarówno zgody niezbędne do realizacji danej usługi lub umowy, jak i takie, które są tylko dodatkiem. Załóżmy, że tworzysz nową aplikację do edycji zdjęć. Aby lepiej działała, wiążesz ją z lokalizacją GPS. W takiej sytuacji nie możesz uzależnić możliwości korzystania z aplikacji od wyrażenia zgody na przetwarzanie danych z lokalizacji, bo nie jest ona konieczna do tego, aby móc korzystać z aplikacji. Choć oczywiście masz prawo o to zapytać – a użytkownik powinien mieć prawo do odmowy.

Kolejny przykład to klasyczna „zgoda” na wykorzystywanie ciasteczek serwowanych nam razem z treścią strony. Jeśli nie przewidujesz możliwości korzystania ze strony po ich wyłączeniu, wtedy taka zgoda będzie traktowana jako wymuszona. Podobnie ma się kwestia zgody na przetwarzanie danych zaszytej w regulaminie (polityce prywatności) usługi, którego nie możemy negocjować.

Co natomiast w sytuacji, kiedy administrator występuje z pozycji władzy i trudno mu odmówić? To może dotyczyć pracodawcy (np. pytającego o zgodę na zbieranie danych, żeby monitorować jakość pracy), szkoły (np. proszącej rodziców o zgodę na kontaktowanie się za pośrednictwem konkretnej aplikacji) czy organu publicznego (np. ośrodka pomocy społecznej proszącego o zgodę na zebranie danych wrażliwych). Tam, gdzie pojawia się presja silniejszego, nie ma miejsca na dobrowolność. A zatem dane powinny być przetwarzane w oparciu o inne podstawy prawne (np. przepis prawa).

Zgoda świadoma i jednoznaczna

Według RODO zgoda wymaga świadomego działania i nie może być wyinterpretowana z milczenia. To ważna zmiana, bo do tej pory wiele firm internetowych zbierało dane właśnie w oparciu o domniemanie, że milczenie/brak działania oznacza zgodę. A przecież to, że nie zmieniamy domyślnych ustawień przeglądarki czy portalu społecznościowego, wcale nie oznacza, że je akceptujemy. Mamy prawo tam po prostu nie zaglądać.

Jak to może wyglądać w praktyce? W naszym cyfrowym życiu zgoda na przetwarzanie danych najczęściej polega na zaznaczeniu okienka wyboru albo przesunięciu suwaka w tzw. ustawieniach prywatności (z „nie” na „tak”). Ale zgodne z prawem jest też wyrażenie zgody poprzez działanie, np. wpisanie swojego adresu e-mail w formularz internetowy, jeśli użytkownik został poinformowany, że robiąc to, akceptuje przetwarzanie swoich danych osobowych w celach marketingowych. Grunt, żeby nie było wątpliwości, że użytkownik właśnie dał Ci zielone światło. W żadnym wypadku nie może zostać uznane za zgodę na przetwarzanie danych jego milczenie lub niepodjęcie żadnych działań (np. zignorowanie irytującego pop-upu na stronie, nieprzestawienie domyślnych ustawień na stronie z „tak” na „nie”).

Możesz przyjąć dowolny sposób wyrażenia zgody: przesunięcie palcem po ekranie, machnięcie ręką przed inteligentną kamerą, obrócenie smartfona zgodnie z ruchem wskazówek zegara lub zataczanie ósemek. Ważne, aby użytkownik miał jasność, że wykonując konkretny ruch lub gest, wyrazi zgodę w odpowiedzi na konkretne zapytanie. Do takich metod nie zalicza się wyrażanie zgody przez przewijanie tekstu zawierającego zapytanie, ponieważ użytkownik, przyzwyczajony do przewijania na ekranie dużej ilości tekstu, może ten fakt łatwo pominąć.

Gdzie to wszystko upchnąć?

RODO wprowadza sporo nowych obowiązków informacyjnych. Po 25 maja zobowiąże Cię do podania następujących informacji:

- tożsamość administratora danych oraz jego dane kontaktowe a także – w razie posiadania przedstawiciela – obowiązek podania tożsamości i danych kontaktowych przedstawiciela administratora danych;
- cele przetwarzania danych osobowych (należy także wspomnieć o podstawie prawnej przetwarzania);
- prawnie uzasadnione interesy realizowane przez administratora danych (jeśli dotyczy);
- odbiorców danych osobowych lub ich kategorie (jeśli istnieją);
- okres, przez który będą przetwarzane dane osobowe (retencja danych), a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- prawa osób, których dane dotyczą (żądanie od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych;
- o zamiarze przekazania danych osobowych do państwa trzeciego bądź organizacji międzynarodowych (jeśli dotyczy);
- o możliwościach uzyskania kopii danych osobowych bądź o miejscu udostępniania tych danych;
- o inspektorze danych osobowych (o ile został wyznaczony);
- o prawie wniesienia skargi do organu nadzorczego;
- o tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym, lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- o profilowaniu.

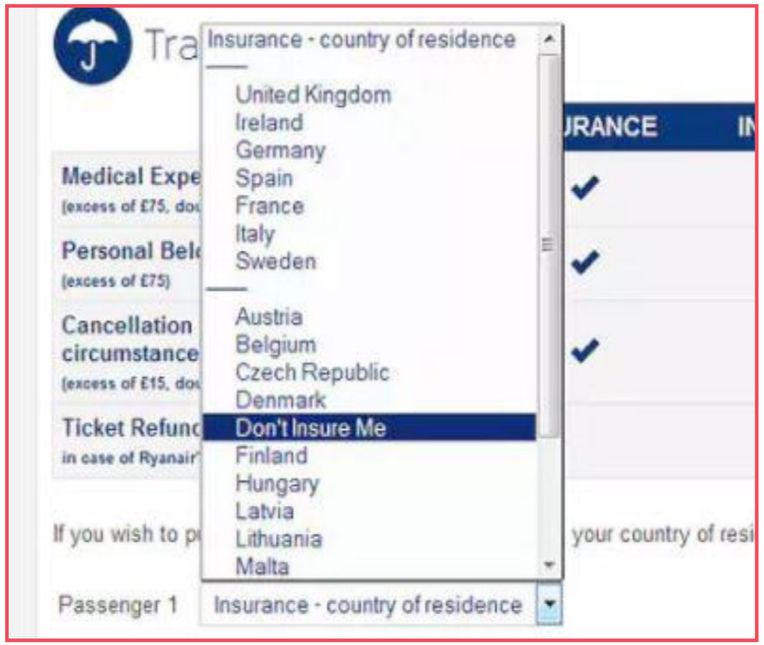
Jak wspomnieliśmy we wcześniejszej części e-booka, wszystkie te informacje muszą być łatwo dostępne. Oczywiście nie oznacza to konieczności tworzenia pop-upów na pół strony, gęsto zapisanych małym drukiem. Jeśli zbierasz dane przez internet, możesz przenieść powyższe informacje na oddzielną stronę (poświęconą polityce prywatności), gdzie możesz przedstawić wszystkie powyższe informacje, dbając jednak o to, aby przy pozyskiwaniu zgody zamieścić do tejże strony wyraźny odnośnik. A jeśli uda Ci się wszystko zwięźle sformułować, możesz się zdecydować na pop-up.

FUNDACJA PANOPTYKON

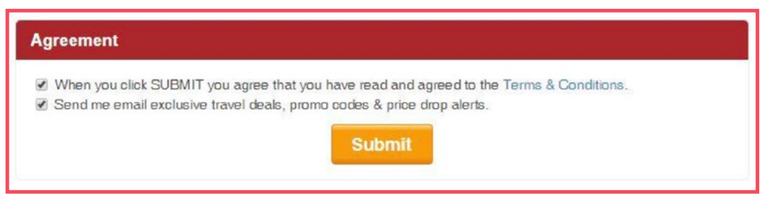
Zgoda – przykłady dobrych i złych praktyk

Zapytanie o zgodę musi zostać przedstawione tak, by dało się je wyraźnie odróżnić od pozostałych kwestii (a więc NIE w ogólnych warunkach czy w polityce prywatności!).

BLEF: Wyszukiwarka lotów, która domyślnie próbuje nas ubezpieczyć



BLEF: Ten portal postanowił wyrazić zgodę za nas. Wystarczy kliknąć „Wyślij”

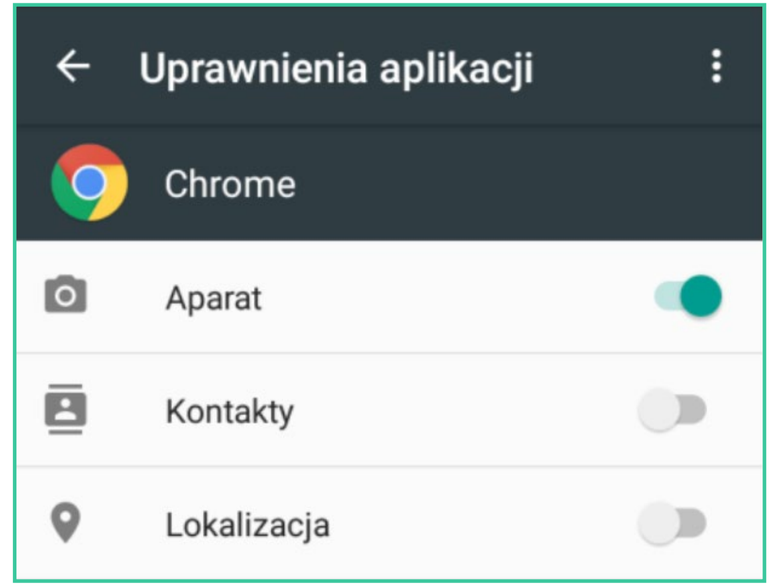


FAIR PLAY

Prosto, zrozumiale i całkiem szczegółowo. Zmieściła się nawet informacja o prawie do cofnięcia zgody!

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie (przykład: *preference management tools*).

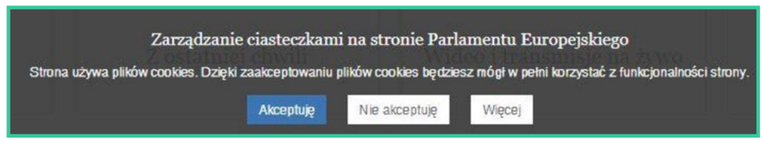
FAIR PLAY: Ruchem palca możemy cofnąć uprawnienia aplikacji



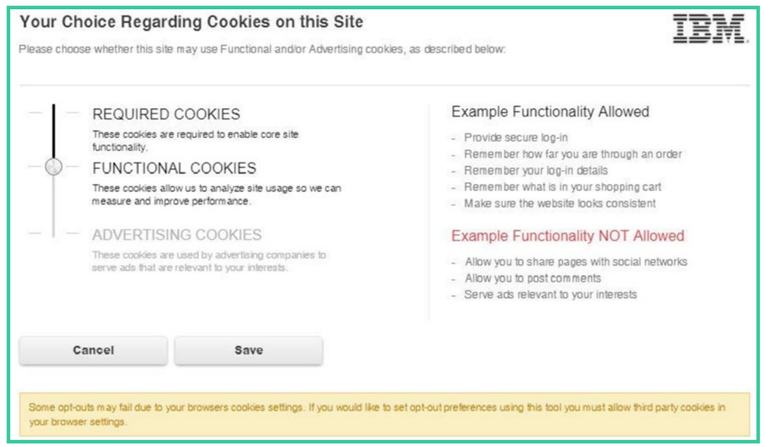
Użytkownik podaje dane dobrowolnie, tj. wykonanie umowy (w tym świadczenie usługi) nie zależy od udzielenia zgody na przetwarzanie danych – o ile przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

BLEF: Wiele portali nadal nie pozwala wyłączyć zapisywania ciasteczek

FAIR PLAY: Możemy się nie zgodzić na zapisywanie ciasteczek



FAIR PLAY: Możemy ustawić, na jakiego typu ciasteczka się godzimy*

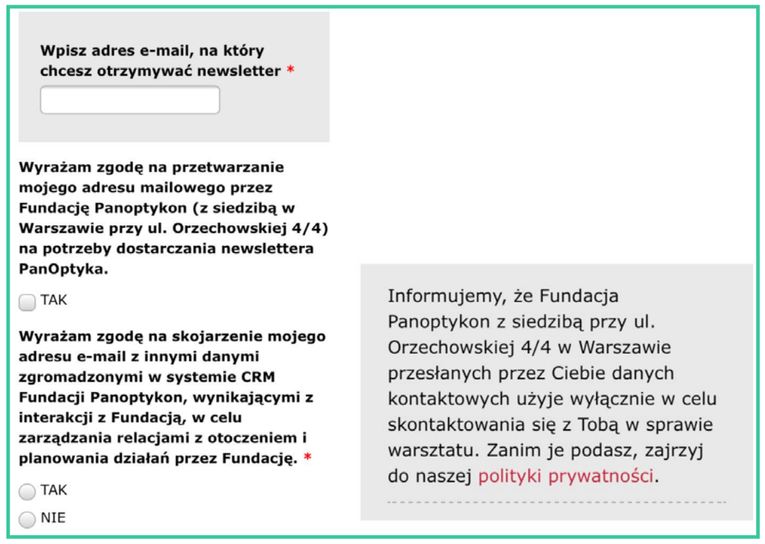


* Niestety strona domyślnie sugeruje zgodę na wszystkie ciasteczka.

FAIR PLAY: Możemy nawet wybrać ciasteczka konkretnych domen, które są wpięte w witrynę

Wyjaśnij, po co Ci te dane: „Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele". Trudne do spełnienia w biznesie reklamowym…

FAIR PLAY:



Nie dla irytujących blokad funkcjonalności! Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na zapytanie elektroniczne, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

BLEF:

Opracowanie redakcyjne

Prowly

Prowly to aplikacja do działań *public relations* dla agencji, firmowych działów komunikacji i freelancerów. Prowly umożliwia sprawne tworzenie biur prasowych online wraz z informacjami prasowymi, artykułami czy postami oraz ich dystrybucję do mediów i pomiar efektów. Z platformy korzysta już kilka tysięcy profesjonalistów z Polski, Europy i Stanów Zjednoczonych, a wśród nich członkowie zespołów PR takich marek, jak Vimeo, Grupa Pracuj, Techland, Deloitte Digital, IKEA, Spotify, National Geographic czy Allegro. Prowly należy do European Tech Alliance i wraz z największymi gigantami technologicznymi z Europy (King, Spotify, BlaBlaCar, Deezer) wspiera Komisję Europejską w budowie strategii jednolitego rynku cyfrowego (DSM).

Partnerzy merytoryczni

FUNDACJA PANOPTYKON

Fundacja Panoptykon jest jedyną organizacją w Polsce, która patrzy na ręce urzędom, służbom, korporacjom – wszystkim tym, którzy zbierają i wykorzystują dane o ludziach, aby na nich wpływać. Od 2009 roku śledzimy tworzone prawo, interweniujemy w obronie praw człowieka, wyjaśniamy zasady działania komercyjnych i państwowych narzędzi nadzoru, przekazujemy praktyczną wiedzę. Dziś dane to waluta i narzędzie władzy: łatwo stracić nad nimi kontrolę. Ale nie tylko. Wszechobecny nadzór karmi lęki i niszczy społeczne zaufanie. Decyzje podejmowane przez algorytmy wzmacniają stereotypy, prowadzą do wykluczenia i dyskryminacji. Naszą misją jest pomaganie ludziom w odzyskaniu kontroli nad swoimi danymi i budowa społeczeństwa, które ceni wolność.

Partnerzy medialni

PR BEZ KRAWATÓW

ZFPR | ZWIĄZEK FIRM PUBLIC RELATIONS

wirtualnemedia

SZAPIRO | SCHWANN PUBLIC RELATIONS

Ma wieloletnie doświadczenie w budowaniu wizerunku korporacyjnego, działaniach *public affairs*, nawiązywaniu dialogu z interesariuszami oraz we współpracy z mediami. Łączy kompetencje agencji i think tanku działającego w obszarze *public relations*.

JSLEGAL JANKOWSKI & STROIŃSKI

Kancelaria założona przez adwokatów dr. Rafała Stroińskiego oraz Bartłomieja Jankowskiego. Zapewnia pełen zakres usług prawniczych, realizowanych poprzez zespoły wyspecjalizowane w obsłudze branż innowacji, IT, finansowej, nieruchomości, logistycznej i nowych technologii, ze szczególnym uwzględnieniem zaawansowanego doradztwa przy rozstrzyganiu sporów oraz doradztwa transakcyjnego i podatkowego. Należy do czołowych polskich kancelarii obsługujących fuzje i przejęcia (w tym transakcje *Private Equity* i *Venture Capital*) oraz wspierających postępowania litygacyjne.

Case studies

MULTI COMMUNICATIONS

KAMIKAZE ALTAVIA GROUP

Redakcja:
Edyta Kowal
Content Marketing Manager & Editor, Prowly

Karol Schwann
Director of Operations,
Szapiro Schwann Public Relations

Korekta:
Magdalena Hutny

Skład:
Marta Olczak
Design Lead, Prowly

Kontakt

Edyta Kowal
Prowly Magazine
e-mail: edyta@prowly.com
tel.: +48 602 684 731

Pamiętaj: nowe zasady ochrony danych osobowych będą dotyczyć także zarządzania bazami mediów

U nas to prostsze, niż myślisz

Moduł RODO/GDPR w Prowly

SPRAWDŹ

Prowly