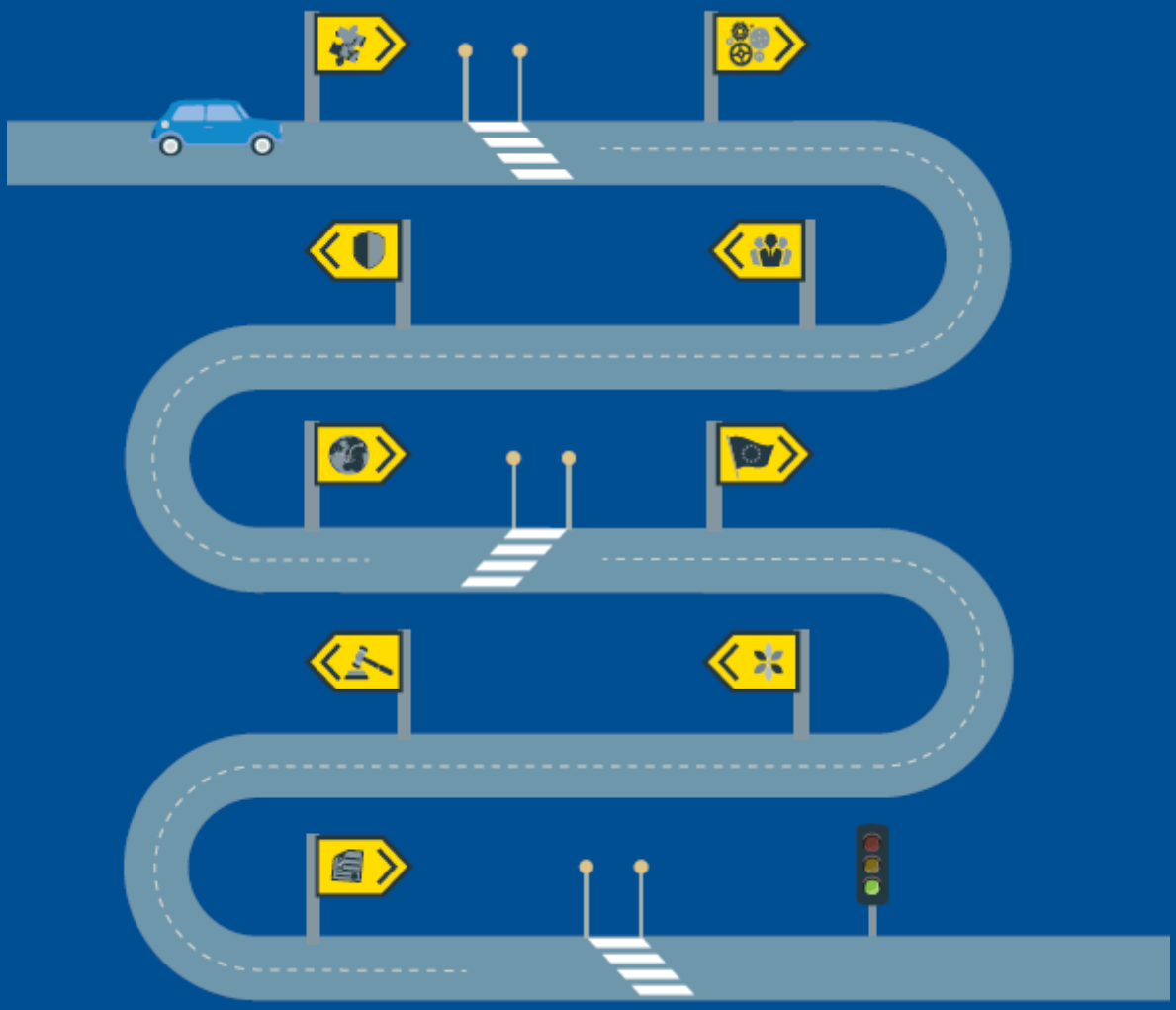
Bird & Bird &

Przewodnik po ogólnym rozporządzeniu o ochronie danych

Październik 2017 roku



Wydając w styczniu 2012 roku projekt ogólnego rozporządzenia o ochronie danych („RODO"), Komisja Europejska rozpoczęła czteroletni cykl debat, rokowań i lobbingu w skali nieznanej dotąd w całej historii Unii Europejskiej. Niniejszy przewodnik podsumowuje przepisy Rozporządzenia, które jest rezultatem tych działań i które w znacznym stopniu zmieni podwaliny unijnego prawa w zakresie ochrony danych w czasie, gdy systemy informatyczne i cyfrowe formy działalności gospodarczej stają się naszą codziennością.

Zmiany, które zostaną wprowadzone przez RODO od piątku 25 maja 2018 roku są znaczące. Liczące ponad 200 stron rozporządzenie jest jednym z najbardziej rozległych źródeł prawa, jakie Unia Europejska uchwaliła w ostatnich latach a pojęcia takie, jak „prawo do bycia zapomnianym," przenoszalność danych, zgłaszanie naruszeń ochrony danych osobowych i rozliczalność (lista jest znacznie dłuższa) będą wymagać czasu, aby się do nich przyzwyczaić. Sam nawet rodzaj aktu prawnego, tj. rozporządzenie, nie zaś dyrektywa - sprawia, że RODO jest dla prawników zajmujących się ochroną danych osobowych instrumentem wyjątkowym.

Niniejszy przewodnik podsumowuje najważniejsze zmiany, które wprowadza nowe prawo, a także zwraca uwagę na najważniejsze działania, jakie należy podjąć w celu spełnienia przewidzianych w nim wymogów.

Nasz przewodnik jest podzielony na rozdziały odpowiadające poszczególnym częściom rozporządzenia, które zostały dodatkowo podzielone tematycznie na podrozdziały. Każdy z podrozdziałów rozpoczyna się od krótkiego streszczenia, proponowanej listy najważniejszych działań, a także naszej oceny stopnia ingerencji, jaką niesie za sobą omawiana część RODO (ocena jest zaprezentowana graficznie jako barometr, który pokazuje pola od zielonego, czyli zmiana niewielkiego stopnia, do czerwonego, co oznacza, że zmiana jest znaczna). Ponadto w każdym z podrozdziałów dodaliśmy grafikę drogowskazu, który pokazuje, gdzie można znaleźć odnośne treści w tekście rozporządzenia. Niniejsza wersja przewodnika uwzględnia wytyczne opublikowane przez Grupę Roboczą w kwietniu 2017 r.

Europejskie prawo ochrony danych jest nieodmiennie przepełnione specyficznym żargonem i charakterystycznymi pojęciami, czego RODO także jest przykładem. Aby pomóc w rozumieniu tego języka zamieściliśmy dodatkowo słowniczek najważniejszych pojęć, który mogą Państwo znaleźć na końcu przewodnika.

Ze względu na fakt, że prawodawcy, organy nadzorcze i sądy są źródłem coraz to nowych wskazówek odnośnie do stosowania RODO, będziemy sukcesywnie aktualizować nasz przewodnik i publikować porady dotyczące nowego prawa. Jeśli chcą Państwo dowiedzieć się więcej na ten temat, prosimy o kontakt. Tymczasem mamy nadzieję, że niniejszy Przewodnik okaże się dla Państwa przydatny.

Ruth Boardman
Partner, UK

James Mullock
Partner, UK

Ariane Mole
Partner, FR

Opracowanie wersji polskiej:

Izabela Kowalczuk-Pakuła, *Senior Associate,*

Szef praktyki ochrony prywatności i danych osobowych

Marian Giersz, *Associate*

Maria Guzewska, *Associate*

Spis treści

Zakres materialny i terytorialny

Na pierwszy rzut oka

- W porównaniu do Dyrektywy 95/46/WE („dyrektywa w sprawie ochrony danych"), którą zastępuje, RODO ma za zadanie rozszerzyć zakres unijnych przepisów o ochronie danych osobowych.
  - Administrator i podmiot przetwarzający z siedzibą na terytorium UE podlegają jego zakresowi – o ile dane osobowe są przetwarzane „w związku z ich działalnością", co jest postanowieniem interpretowanym w sposób szeroki.
  - W przypadku braku przedstawicielstwa na terytorium UE, RODO nadal ma zastosowanie w przypadku, gdy: (1) dane osobowe osoby zamieszkującej na terytorium UE są przetwarzane w związku z oferowaniem tej osobie towarów lub usług; lub (2) gdy zachowania osób w UE są „monitorowane".
- Pomimo formy rozporządzenia, RODO pozwala państwom członkowskim na stanowienie własnego prawa w wielu obszarach. Będzie to stać w sprzeczności z celem tego aktu prawnego, którym jest ujednolicenie przepisów.
- RODO nie ma zastosowania do niektórych czynności - w tym do przetwarzania danych na mocy dyrektywy o organach ścigania, dla celów bezpieczeństwa narodowego, a także przetwarzania danych przez osoby fizyczne wyłącznie w ramach działalności o charakterze osobistym/ domowym.
- RODO będzie miało zastosowanie od 25 maja 2018 roku.

Co trzeba zrobić

Organizacje nieposiadające przedstawicielstwa na terenie UE, których działania dotyczą obywateli UE, powinny:

- zdawać sobie sprawę z wpływu RODO;

oraz

- opracować własne podejście do kwestii zgodności z jego przepisami

Organizacje działające w obszarach, w których zastosowanie znajdują zasady „szczególne/sektorowe", powinny:

- samodzielnie ocenić, czy potrzebują określonych przepisów krajowych i dążyć do ich uchwalenia w razie potrzeby; a także
- uważnie śledzić postępy w ich przygotowywaniu na wypadek, gdyby miały zostać uchwalone w sposób niekorzystny dla tych organizacji.

Zakres terytorialny

Administratorzy i podmioty przetwarzające dane posiadający jednostkę organizacyjną w UE

RODO będzie mieć zastosowanie do organizacji, które posiadają na terytorium Unii *„jednostki organizacyjne”*, w przypadku, gdy przetwarzanie danych osobowych odbywa się *„w związku z działalnością”* tej jednostki.

Jeśli to kryterium będzie spełnione, RODO będzie mieć zastosowanie bez względu na to, czy przetwarzanie danych faktycznie odbywa się na terytorium UE.

Pojęcie *„jednostki organizacyjnej”* było przedmiotem rozważań Trybunału Sprawiedliwości Unii Europejskiej („TSUE”) w sprawie z 2015 r. *Weltimmo* v. *NAIH* (C-230/14). Potwierdzono wtedy, że jednostka organizacyjna jest *„szerokim”* i *„elastycznym”* pojęciem, którego znaczenie nie powinno zależeć od formy prawnej. Można uznać, że dana organizacja posiada *„jednostkę organizacyjną”* w przypadku, gdy prowadzi *„faktyczną lub przynoszącą efekty działalność - nawet na minimalną skalę”* - dzięki *„trwałym rozwiązaniom organizacyjnym”* na terytorium Unii. Wystarczająca może być obecność jednego przedstawiciela. W sprawie tej uznano, że Weltimmo posiada jednostkę organizacyjną na terytorium Węgier ze względu na prowadzenie strony internetowej w języku węgierskim, na której reklamowane były nieruchomości zlokalizowane na Węgrzech (co oznaczało, że w rezultacie działalność została uznana za *„głównie lub całkowicie nakierowaną na to państwo* członkowskie”), korzystanie z usług lokalnego agenta, (który odpowiadał za windykację należności na lokalnym rynku i działał w charakterze pełnomocnika w postępowaniach administracyjnych i sądowych), oraz korzystanie z węgierskiego adresu korespondencyjnego i konta bankowego dla celów gospodarczych - bez względu na to, że spółka Weltimmo została założona na Słowacji.

Organizacje posiadające biura sprzedaży na terytorium UE, które zajmują się promowaniem lub sprzedażą usług w zakresie reklamy i promocji, których celem są obywatele UE, z dużym prawdopodobieństwem będą podlegać przepisom RODO ze względu na fakt, że przetwarzanie danych osobowych w ramach ich działalności jest uznawane za *„nierozerwalnie związane”* z działalnością, a także prowadzone *„w ramach działalności”* wspomnianej jednostki organizacyjnej znajdującej się na terytorium UE *(Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (C-131/12).

Organizacje nieposiadające „jednostki organizacyjnej” w UE, których działalność dotyczy mieszkańców Unii lub które ich monitorują

Organizacje nieposiadające jednostki organizacyjnej w UE będą podlegać przepisom RODO w przypadku, gdy przetwarzają dane osobowe mieszkańców Unii w związku z:

- *„oferowaniem towarów i usług”* (odpłatność nie jest warunkiem); lub
- *"monitorowaniem”* ich zachowania na terytorium Unii.

Nie wystarczy sama dostępność strony internetowej na terytorium UE. Należy ustalić, że dana organizacja *„przewiduje”*, iż jej działania będą dotyczyły także osób znajdujących się w Unii.

Adresy kontaktowe dostępne z terytorium UE i posługiwanie się językiem państwa administratora danych także nie są wystarczające. Jednakże posługiwanie się językiem/walutą państwa członkowskiego UE, możliwość składania zamówień w tym języku i odniesienia do użytkowników lub klientów z terytorium Unii będą miały znaczenie.

TSUE dokonał analizy tego, kiedy działalność (np. oferowanie towarów i usług) będzie uznana za *„nakierowaną na”* państwa członkowskie Unii w innym kontekście (tj. na mocy Rozporządzenia „Bruksela 1” (44/2001/WE) dotyczącego *„jurysdykcji ... w sprawach cywilnych i handlowych”*). Jego uwagi prawdopodobnie pomogą w wykładni w niniejszym, podobnym aspekcie RODO. Oprócz powyższych rozważań, TSUE zwraca uwagę na fakt, że zamiar podejmowania działań w odniesieniu do konsumentów z terytorium Unii może być wykazany przez: (1) *„niezaprzeczalny”* dowód, np. uregulowanie opłaty na rzecz właściciela wyszukiwarki internetowej w zamian za ułatwienie dostępu osobom z terytorium danego państwa członkowskiego lub z listy państw członkowskich; a także (2) inne czynniki - także w połączeniu, np. *„międzynarodowy charakter”* danej działalności (w tym niektóre usługi turystyczne), wzmianki o numerach telefonu z międzynarodowym kodem, korzystanie z domeny najwyższego poziomu, nie zaś z rozszerzenia właściwego dla państwa, w którym uczestnik rynku posiada jednostkę organizacyjną (np. .de lub .eu), opis *„tras przejazdu ... z państw członkowskich do miejsca, w którym świadczone są usługi”*, a także wzmianki o *„międzynarodowej klienteli składającej się z klientów zamieszkujących w różnych państwach członkowskich”*. Lista *nie jest wyczerpująca* i odpowiedź na to pytanie zależy od przypadku *(Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller* (połączone sprawy (C-585/08) i (C-144/09)).

Istnieją wątpliwości co do tego czy jednostki organizacyjne spoza UE oferujące towary i usługi przedsiębiorstwom (z wyłączeniem osób fizycznych) mającym siedziby w UE wejdą w zakres testu „oferowania towarów i usług” przewidzianego w art. 3(2)(a) RODO.

„Monitorowanie” obejmuje w szczególności śledzenie osób w internecie w celu profilowania, także w przypadku wykorzystywania tej techniki do analizowania/przewidywania preferencji, zachowań i nastawienia.

Organizacje podlegające szerokiej właściwości przepisów RODO są zobowiązane do powołania przedstawiciela na terytorium UE.

Na mocy dyrektywy w sprawie ochrony danych organizacje, których działalność dotyczy osób zamieszkujących terytorium UE musiały przestrzegać unijnych przepisów tyko w przypadku, gdy wykorzystywały na terytorium Unii *„środki”* do przetwarzania danych osobowych. Przez to krajowe organy nadzorcze, których celem było zabezpieczenie swojej jurysdykcji, wypracowały stanowisko, według którego wykorzystywanie plików cookie, a także zachęcanie użytkowników do wypełniania formularzy, było równoznaczne z wykorzystywaniem na terytorium Unii *„środków”* do przetwarzania danych. Po wprowadzeniu nowych przepisów łatwiej będzie wykazać zastosowanie unijnego prawa (jednakże w przypadku, gdy dana organizacja nie posiada jednostki organizacyjnej na terytorium UE, egzekwowanie nowych przepisów może okazać się trudne jak dotychczas).

W przypadkach, gdy prawo państwa członkowskiego UE ma zastosowanie z mocy prawa międzynarodowego publicznego

Motyw 25 zawiera przykład misji dyplomatycznej lub stanowiska konsularnego.

Wyłączenia

Niektóre formy działalności są całkowicie wyłączone z zakresu RODO (wykaz poniżej).

Ponadto, RODO uwzględnia fakt, że przepisy o ochronie danych nie mają charakteru absolutnego i należy je stosować w sposób wyważony (proporcjonalny) w stosunku do innych regulacji - w tym w zakresie *„wolności prowadzenia działalności gospodarczej”* (informacje na temat prawa państw członkowskich do wprowadzania odstępstw znajdują się w części poświęconej wyjątkom i warunkom szczególnym. Ze względu na fakt, że RODO zaostrza prawo w wielu obszarach ochrony danych poprzez wprowadzenie większej ilości obowiązków w stosunku do zachęt, powyższe stwierdzenie z Motywu 4 może się okazać przydatne w przyszłości, zwłaszcza dla przedsiębiorców.

RODO nie ma zastosowania do przetwarzania danych osobowych (te ogólne wyłączenia są bardzo podobne do odpowiednich przepisów dyrektywy w sprawie ochrony danych):

- w ramach działalności nieobjętej zakresem prawa UE (np. działalności w zakresie bezpieczeństwa narodowego);
- w odniesieniu do wspólnej polityki zagranicznej i bezpieczeństwa UE;
- przez właściwe organy publiczne dla celów zapobiegania, prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępczości i związanych z tym kwestii (tam, gdzie obecnie ma zastosowanie dyrektywa o organach ścigania (UE)[1] 2016/680, która została przyjęta 26 kwietnia 2016 r.);
- przez instytucje UE w przypadku, gdy Rozporządzenie 45/2001/WE będzie nadal stosowane zamiast RODO. To rozporządzenie zostanie uaktualnione w celu zapewnienia jego spójności z RODO; a także
- przez osobę fizyczną w ramach *„czynności o czysto osobistym lub domowym charakterze”*. Powyższe obejmuje korespondencję i przechowywanie adresów - ale obecnie także podtrzymywanie więzi społecznych i działalność internetową podejmowaną dla celów społecznych i domowych. Wskazuje to na możliwość poszerzenia zakresu odstępstwa istniejącego na mocy zasad określonych w *Bodil Lindqvist* (C-101/01) jeszcze przed nadejściem mediów społecznościowych. W tym przypadku TSUE zauważył, że udostępnianie danych w internecie bez ograniczeń *„w taki sposób, że dane te są dostępne nieograniczonemu gronu osób”* nie może mieścić się w zakresie tego odstępstwa, które powinno być ograniczone do działań *„podejmowanych w ramach czynności o charakterze prywatnym lub rodzinnym przez osoby fizyczne”*. Należy także zwrócić uwagę, że RODO nadal będzie mieć zastosowanie do administratorów i podmiotów przetwarzających dane, którzy *„udostępniają środki przetwarzania danych”*, co mieści się w zakresie tego odstępstwa.

Wprowadzenie RODO powinno pozostać *„bez uszczerbku”* dla regulacji zawartych w dyrektywie dotyczącej handlu elektronicznego (2000/31/WE), w szczególności w odniesieniu do tych przepisów, które dotyczą odpowiedzialności *„usługodawców będących pośrednikami”* (oraz tych, które mają na celu ograniczenie ich ekspozycji na odpowiedzialność o charakterze karnym i finansowym w przypadku, gdy ich działalność ogranicza się do „hostingu”, „cachingu” lub ma postać *„zwykłego przekazu”*). Związek z dyrektywą dotyczącą handlu elektronicznego jest złożony ze względu na fakt, że dyrektywa ta stwierdza, że kwestie związane z przetwarzaniem danych nie są objęte jej zakresem i *„podlegają wyłącznie”* właściwym przepisom o ochronie danych. Oba akty prawne można interpretować w sposób spójny przy założeniu, że odpowiedzialność dostawców usług internetowych za działania użytkowników będzie określana na mocy przepisów dyrektywy dotyczącej handlu elektronicznego, ale inne kwestie (np. obowiązki w zakresie usuwania lub sprostowania danych, lub też obowiązki ciążące na dostawcach usług internetowych w zakresie wykorzystywania przez nich danych osobowych) będą podlegać przepisom RODO. Kwestia ta nie jest jednak oczywista.

Rozporządzenie kontra prawo krajowe

Jako rozporządzenie, RODO będzie obowiązywać bezpośrednio w państwach członkowskich bez potrzeby uchwalania przepisów implementujących.

W wielu jednak przypadkach RODO pozwala państwom członkowskim na uchwalenie własnego prawa w zakresie ochrony danych. Powyższe obejmuje sytuacje, w których przetwarzanie danych osobowych jest konieczne w celu wypełnienia obowiązku prawnego, odnosi się do interesu publicznego lub jest realizowane przez organy publiczne. Wiele artykułów może być dodatkowo doprecyzowywane lub ograniczone przez przepisy prawa danego państwa członkowskiego.

Organizacje działające w sektorach, które często podlegają *szczególnym sytuacjom związanym z przetwarzaniem (np. służba zdrowia, usługi finansowe)* powinny: (1) rozważyć czy wspomniane szczególne sytuacje, które mogą być doprecyzowywane lub uogólnione w stosunku do przepisów RODO, będą dla nich korzystne; oraz (2) popierać te, które zostaną uznane za najbardziej sprzyjające. Powinny także monitorować działalność państw członkowskich zamierzających wprowadzić *szczególne sytuacje*, które mogą skutkować dodatkowymi ograniczeniami lub okazać się niespójne z przepisami innych państw członkowskich.

Gdzie mogę to znaleźć?

Zakres przedmiotowy	*art. 2, motywy 3, 15-21*
Zakres terytorialny	*art. 3, motywy 22-25*

[1] Pełny tytuł: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW

Nowe lub zmienione pojęcia

Na pierwszy rzut oka

RODO wprowadzi znaczne zmiany między innymi dzięki następującym pojęciom:

- *Przejrzystość i Zgoda* - tj. informacje, które należy przekazać i zgody, które należy uzyskać od osób, których dane dotyczą, w celu uzasadnienia wykorzystywania tych danych. Wymogi RODO, w tym w zakresie zgody, która musi być jednoznaczna i nie może być domniemana na podstawie braku działania, oznaczają, że wiele informacji przekazanych osobom fizycznym dotyczących ochrony danych będzie wymagało poprawek.
- *Dzieci i zgoda* - wyrażona cyfrowo zgoda rodziców wymagana jest w przypadku wykorzystywania danych osoby poniżej 13 roku życia. Państwa członkowskie mają swobodę ustanawiania własnych zasad w odniesieniu do osób w wieku od 13 do 15 lat (włącznie). Jeśli jednak nie skorzystają z tego prawa, zgoda rodziców będzie wymagana dla wszystkich dzieci poniżej 16 roku życia.
- *Dane regulowane* - definicje „danych osobowych" i „danych wrażliwych" zostały rozszerzone, dla przykładu ta ostatnia obejmuje teraz dane genetyczne i biometryczne.
- *Pseudonimizacja* - technika zwiększająca ochronę prywatności polegająca na tym, że informacje pozwalające na przypisanie danych do określonych osób są przechowywane oddzielnie i z zastosowaniem technicznych i organizacyjnych środków zapewniających, że dane nie zostaną ze sobą skojarzone.
- *Naruszenie ochrony danych osobowych* - nowe obowiązki w zakresie powiadamiania o naruszeniu bezpieczeństwa danych zostaną wprowadzone w odniesieniu do wszystkich administratorów danych, bez względu na sektor.
- *Uwzględnianie ochrony danych w fazie projektowania i rozliczalność* - organizacje mają obowiązek wdrożenia znacznej liczby nowych środków technicznych i organizacyjnych w celu wykazania zgodności z RODO.
- *Zwiększone prawa* – osoby, których dane dotyczą, otrzymują nowe, szersze uprawnienia, w tym prawo do bycia zapomnianym, prawo do przenoszenia danych i prawo do sprzeciwu wobec zautomatyzowanego podejmowania decyzji.
- *Współpraca miedzy organem nadzorczym a Europejską Radą Ochrony Danych* - nadzór regulacyjny nad ochroną danych ulegnie zmianie w znacznym stopniu, w tym na skutek m.in. wprowadzenia organów wiodących dla niektórych jednostek organizacyjnych.

Co trzeba zrobić

Nie ma potrzeby podejmowania żadnych działań.

Przepisy RODO i obowiązki, jakie na jego gruncie powstają są szeroko zakrojone, ale poniższe pojęcia szczególnie wyraźnie jawią się jako nowe lub znacznie zmienione koncepcje. Więcej informacji o każdym z tych pojęć znajdą Państwo w innych miejscach w niniejszym przewodniku.

Zgoda

Warunki uzyskania zgody uległy zaostrzeniu:

- osoba, której dane dotyczą, ma prawo wycofać zgodę w dowolnym momencie; a także
- dla różnych działań w zakresie przetwarzania danych wymagane są osobne zgody; ponadto zgody wymuszone lub ogólne mechanizmy wyrażania zgody nie będą akceptowalne. Wkrótce powinno się pojawić więcej wytycznych, ale już teraz wiadomo, że organizacje będą musiały dokonać przeglądu swoich mechanizmów wyrażania zgody, aby zapewnić możliwość dokonania rzeczywistego i każdorazowego wyboru.

Zgoda nie jest jednak jedynym mechanizmem uprawniającym do przetwarzania danych osobowych. Pojęcia takie, jak niezbędność do wykonania umowy, wypełnienie obowiązku prawnego (krajowego bądź unijnego), lub przetwarzanie w związku z prawnie uzasadnionym interesem, będą nadal funkcjonować.

Więcej informacji na ten temat znajdą Państwo w częściach poświęconych zgodzie; dzieciom oraz danym wrażliwym i przetwarzaniu zgodnie z prawem (rozdział poświęcony zasadom).

Przejrzystość

Organizacje będą musiały dostarczać osobom, których dane dotyczą, obszernych informacji na temat przetwarzania ich danych osobowych.

RODO łączy w sobie różne obowiązki w zakresie przejrzystości, które funkcjonują w UE. Wykaz informacji, jakich należy dostarczyć, zajmuje w tekście RODO 6 stron, jednak administratorzy danych muszą sami zrobić to, co nie udało się unijnemu prawodawcy, tj. dostarczyć informacji w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny.

RODO przewiduje możliwość korzystania ze standardowych znaków graficznych, dając Komisji możliwość dokonania wyboru i wprowadzenia takich znaków za pomocą aktów delegowanych na późniejszym etapie.

Więcej informacji na ten temat znajduje się w części poświęconej informacjom dla osób, których dane dotyczą.

Dzieci

Dzieci poniżej 13 roku życia w żadnym przypadku nie mogą samodzielnie wyrazić zgody na przetwarzanie ich danych osobowych w odniesieniu do usług świadczonych w internecie.

W przypadku dzieci w wieku od 13 do 15 lat (włącznie), obowiązuje generalna zasada, według której jeśli dana organizacja ubiega się o zgodę na przetwarzanie ich danych osobowych, należy uzyskać zgodę rodzica, chyba że dane państwo członkowskie obniży, poprzez uchwalenie odpowiednich przepisów, odpowiedni próg wieku, przy czym próg ten w żadnym przypadku nie może spaść poniżej 13 lat.

Dzieci w wieku 16 lub więcej lat mogą wyrazić zgodę na przetwarzanie danych osobowych we własnym imieniu.

Nie ma żadnych konkretnych zasad odnoszących się do zgody rodzica na przetwarzanie danych osobowych offline: mają tu zastosowanie przepisy krajowe danego państwa członkowskiego.

Więcej informacji na ten temat znajduje się w części poświęconej dzieciom.

Dane osobowe/ dane wrażliwe („szczególne kategorie danych osobowych")

RODO ma zastosowanie do danych, które identyfikują, lub mogą posłużyć (komukolwiek) do zidentyfikowania, żyjącej osoby, pośrednio lub bezpośrednio. W tym zakresie zachowany został test, wprowadzony przez dyrektywę w sprawie ochrony danych, znany jako „*wszystkie środki mogące posłużyć*" do zidentyfikowania.

W Preambule RODO zaznaczono, że niektóre kategorie danych w internecie mogą mieć charakter danych osobowych, odwołując się do przykładów takich, jak identyfikatory internetowe, identyfikatory urządzeń, identyfikatory plików cookie i adresy IP. W sprawie C-582/14 Patrick Breyer / Bundesrepublik Deutschland (wyrok z 19 października 2016 r.) TSUE uznał, że dynamiczny adres IP zarejestrowany przez „dostawcę usług medialnych online" (czyli przez podmiot prowadzący stronę internetową) przy okazji przeglądania strony internetowej, którą dostawca ten udostępnia publicznie, stanowi wobec tego podmiotu dane osobowe, gdy dysponuje on środkami prawnymi umożliwiającymi mu zidentyfikowanie osoby odwiedzającej oraz dzięki dodatkowym informacjom, jakimi dysponuje dostawca usług internetowych osoby odwiedzającej tę stronę internetową. Co istotne, TSUE nie odniósł się do wytycznych Grupy Roboczej mówiących o tym, że wyróżnienie danej osoby na podstawie indywidualnych identyfikatorów dla celów śledzenia zachowania tej osoby w internecie stanowi przetwarzanie danych osobowych (Opinia 188). Podmioty prowadzące internetową reklamę behawioralną powinny mieć świadomość, że zgodnie z Motywem 30 RODO takie indywidualne identyfikatory użyte do tworzenia profili w celu identyfikowania osób będą stanowiły dane osobowe.

Pojęcie „szczególnych kategorii danych osobowych" (często nazywanych danymi wrażliwymi) zostaje zachowane i rozszerzone o dane genetyczne oraz dane biometryczne. Podobnie, jak w przypadku obecnie obowiązującej dyrektywy w sprawie ochrony danych, przetwarzanie tego rodzaju danych podlega bardziej restrykcyjnym warunkom, niż przetwarzanie innych rodzajów danych osobowych.

Gdzie mogę to znaleźć?
art. 4, motywy różne (zwłaszcza 26-35)

Pseudonimizacja

Jest to nowa definicja, która odwołuje się do techniki przetwarzania danych osobowych w taki sposób, aby nie można ich było przypisać do określonej *„osoby, której dane dotyczą”* bez dodatkowych informacji, które muszą być przechowywane oddzielnie i z zastosowaniem technicznych i organizacyjnych środków zapewniających, że dane nie zostaną ze sobą skojarzone.

Informacje spseudonimizowane nadal stanowią dane osobowe, jednak zaleca się stosowanie tej techniki, w szczególności w przypadku:

- gdy jest to czynnik do rozważenia przy określaniu, czy przetwarzanie jest *„niezgodne”* z celem, dla którego dane osobowe były pierwotnie zbierane i przetwarzane;
- gdy może ona przyczynić się do spełnienia wymogu „uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych” (więcej informacji w części poświęconej obowiązkom w zakresie zarządzania danymi);
- gdy może ona przyczynić się do wypełnienia przewidzianych w RODO obowiązków w zakresie bezpieczeństwa danych (więcej informacji w części poświęconej naruszeniom ochrony danych osobowych i ich zgłaszaniu); oraz
- w przypadku organizacji zamierzających wykorzystywać dane osobowe dla potrzeb badań historycznych lub naukowych, lub też dla celów statystycznych, podkreśla się przydatność techniki pseudonimizacji

Zawiadomienie o naruszeniu ochrony danych osobowych

RODO wprowadza ramy organizacyjne dla systemu zawiadamiania o naruszeniach bezpieczeństwa danych dla wszystkich administratorów danych osobowych bez względu na sektor, w którym działają.

Obowiązki w zakresie zawiadamiania (organów nadzorczych i osób, których dane dotyczą) mogą pojawiać się w rezultacie *„utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”*. Więcej informacji na ten temat znajduje się w części poświęconej naruszeniom ochrony danych osobowych i ich zgłaszaniu.

Uwzględnianie ochrony danych w fazie projektowania / rozliczalność

Organizacje muszą być w stanie wykazać zgodność z przepisami RODO, w tym poprzez przyjęcie pewnych środków w zakresie *„uwzględniania ochrony danych w fazie projektowania”* (np. zastosowanie techniki pseudonimizacji), szkolenia pracowników i przeprowadzania audytów.

W przypadku przetwarzania o „wysokim stopniu ryzyka” (np. monitorowanie, regularne oceny lub przetwarzanie szczególnych kategorii danych osobowych), należy przeprowadzić i udokumentować szczegółową ocenę skutków dla ochrony danych. W przypadku, gdy wynik wyżej wspomnianej oceny wskazuje, że istnieje wysokie i niczym niezminimalizowane ryzyko dla osób, których dane dotyczą, administratorzy danych muszą powiadomić organ nadzorczy i uzyskać jego opinię na temat adekwatności środków zaproponowanych w ocenie skutków dla ochrony danych w celu zmniejszenia ryzyka związanego z przetwarzaniem danych.

Administratorzy i podmioty przetwarzające dane mogą powołać inspektora ochrony danych. Jest to obowiązkowe w przypadku jednostek sektora publicznego oraz podmiotów wykonujących pewne działania o charakterze wrażliwym lub monitorowania oraz gdy prawo krajowe tego wymaga (przykładowo, w Niemczech obowiązek taki najprawdopodobniej będzie obowiązywał również po maju 2018). Spółki powiązane mogą wspólnie powoływać inspektora ochrony danych.

Więcej informacji na ten temat znajduje się w części poświęconej obowiązkom w zakresie zarządzania danymi.

Zwiększone prawa dla osób fizycznych

RODO kładzie szczególny nacisk na zakres istniejących i nowych praw przysługujących osobom fizycznym w odniesieniu do ich danych osobowych.

Prawa te obejmują prawo do bycia zapomnianym, prawo do żądania przeniesienia danych osobowych do nowego usługodawcy, prawo do sprzeciwu wobec niektórych czynności w zakresie przetwarzania danych, oraz prawo do sprzeciwu wobec zautomatyzowanego podejmowania decyzji.

Więcej informacji na ten temat znajduje się w części poświęconej informacjom dla osób, których dane dotyczą.

Organy nadzorcze i EROD

Organy regulacyjne sprawujące nadzór nad kwestiami ochrony danych są określane mianem organów nadzorczych.

Jeden wiodący organ nadzorczy zlokalizowany w państwie członkowskim, w którym dana organizacja posiada główną jednostkę organizacyjną, będzie sprawował nadzór nad przestrzeganiem przepisów RODO przez całą organizację.

Powołana zostanie Europejska Rada Ochrony Danych („EROD”) w celu (między innymi) wydawania opinii w zakresie szczegółowych kwestii i rozstrzygania sporów wynikających z decyzji organów nadzorczych.

Więcej informacji na ten temat znajduje się w części poświęconej prawom przysługującym osobom fizycznym.

Zasady ochrony danych

Na pierwszy rzut oka

- Zasady ochrony danych zostały poddane przeglądowi, są jednak podobne do zasad określonych w dyrektywie w sprawie ochrony danych: rzetelność, zgodność z prawem i przejrzystość; ograniczenie celu; minimalizacja danych; jakość danych; bezpieczeństwo, integralność i poufność.
- Nowa zasada rozliczalności nakłada na administratorów danych odpowiedzialność za wykazanie zgodności z zasadami ochrony danych.

Co trzeba zrobić

Należy dokonać przeglądu polityki ochrony danych, kodeksów postępowania i szkoleń pracowników w celu zapewnienia, że są one zgodne z nowymi zasadami.

Należy określić środki potrzebne do *„wykazania przestrzegania”* - np. przestrzeganie zatwierdzonych kodeksów postępowania, zachowywanie historii podejmowanych decyzji w zakresie przetwarzania danych oraz, w zależności od potrzeb, oceny skutków dla ochrony danych.

Komentarz

Zasady wprowadzone na mocy RODO są podobne do zasad określonych w dyrektywie w sprawie ochrony danych, są jednak pewne nowe elementy, wyróżnione poniżej (zapis kursywą).

Zgodność z prawem, rzetelność i przejrzystość

Dane osobowe muszą być przetwarzane w sposób zgodny z prawem, rzetelnie, a także w *sposób przejrzysty dla osoby, której dane dotyczą.*

Ograniczenie celu

Dane osobowe muszą być zbierane dla określonych, wyraźnych i zgodnych z prawem celów, a ponadto nie mogą być dalej przetwarzane w sposób niezgodny z wyżej wspomnianymi celami. Dalsze przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnym celem przetwarzania. Jednakże warunki przedstawione w art. 89(1), który przewiduje środki ochrony i wyjątki w zakresie przetwarzania danych dla wyżej wspomnianych celów, muszą być spełnione.

Minimalizacja danych

Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane.

Prawidłowość

Dane osobowe muszą być prawidłowe oraz, w razie potrzeby, aktualne; należy podjąć wszelkie środki w celu zapewnienia, że dane osobowe, które są nieprawidłowe w odniesieniu do celu, dla którego są przetwarzane, zostaną bezzwłocznie usunięte lub poprawione.

Ograniczenie przechowywania

Dane osobowe muszą być przetwarzane *w takiej formie, która pozwala na identyfikację osób, których dane dotyczą* tylko przez taki okres, w jakim jest to konieczne z perspektywy celów, dla których dane osobowe są przetwarzane. Dane osobowe mogą być przechowywane przez dłuższy okres, o ile dane te są przetwarzane wyłącznie *do celów archiwalnych w interesie publicznym*, do celów badań naukowych lub historycznych, lub do celów statystycznych zgodnie z art. 89(1), a także pod warunkiem wdrożenia odpowiednich technicznych i organizacyjnych środków bezpieczeństwa.

Integralność i poufność

Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiedni poziom bezpieczeństwa danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz ochronę przed przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych.

Rozliczalność

Administrator jest odpowiedzialny za przestrzeganie wspomnianych przepisów i musi *być w stanie wykazać* zgodność z nimi.

Gdzie mogę to znaleźć?
art. 5, motyw 39

Zgodność z prawem przetwarzania i dalszego przetwarzania

Na pierwszy rzut oka

- Podstawy przetwarzania danych osobowych na mocy RODO są generalnie powieleniem podstaw przewidzianych w dyrektywie w sprawie ochrony danych.
- Wprowadzono nowe ograniczenia wykorzystywania zgody i przetwarzania danych osobowych dzieci w działalności internetowej.
- Istnieją określone ograniczenia możliwości powoływania się na „prawnie uzasadniony interes" jako podstawę przetwarzania danych, a także pewne objaśnienia dotyczące tego kiedy można z tej podstawy korzystać.
- Istnieje niewyczerpująca lista czynników, które należy uwzględnić przy ocenie tego, czy przetwarzanie danych dla nowego celu jest niezgodne z celem, dla którego dane były pierwotnie zbierane

Co trzeba zrobić

- Należy upewnić się, że określili Państwo podstawy zgodnego z prawem przetwarzania danych, na których opiera się działalność Państwa organizacji, a także sprawdzić, czy te podstawy nadal będą ważne po wejściu w życie RODO.
- W przypadku przetwarzania danych na podstawie zgody, należy zapewnić, że wyrażona zgoda spełnia obowiązujące wymogi (więcej informacji na ten temat znajduje się w części poświęconej wyrażaniu zgody).
- Należy rozważyć, czy nowe zasady dotyczące przetwarzania danych dzieci w działalności internetowej będą Państwa dotyczyć, a jeśli tak, jakich krajowych zasad będą Państwo musieli przestrzegać (więcej informacji na ten temat znajduje się w części poświęconej danym dzieci).
- Należy zapewnić, że Państwa wewnętrzne procesy kierownicze umożliwią Państwu wykazanie sposobu, w jaki decyzje o wykorzystywaniu danych do dalszego przetwarzania zostały podjęte, a także tego, że uwzględniono w tym procesie wszystkie istotne czynniki.

Komentarz

Art. 6(1) RODO określa warunki, jakie należy spełnić, aby przetwarzanie danych osobowych było zgodne z prawem (więcej informacji na temat przepisów dotyczących danych wrażliwych znajduje się w części poświęconej danym wrażliwym i przetwarzaniu zgodnie z prawem). Podstawy te są generalnie powieleniem podstaw przewidzianych w dyrektywie w sprawie ochrony danych. Podstawami tymi są:

6(1)(a) – Zgoda osoby, której dane dotyczą

RODO przyjmuje bardziej restrykcyjne podejście do kwestii zgody, m. in. poprzez dążenie do zapewnienia, że zgoda ma charakter odpowiedni dla określonego celu przetwarzania danych (więcej informacji na ten temat znajduje się w części poświęconej zgodzie). Szczególne warunki obowiązują w przypadku dzieci (więcej informacji na ten temat znajduje się w części poświęconej dzieciom).

6(1)(b) – Konieczne dla wykonania umowy zawartej z osobą, której dane dotyczą, lub do podjęcia działań przygotowawczych do zawarcia takiej umowy

Bez zmian w stosunku do przepisów dyrektywy w sprawie ochrony danych.

6(1)(c) – Niezbędne do wypełnienia obowiązku prawnego

Jest to powielenie podstawy prawnej przewidzianej w dyrektywie w sprawie ochrony danych. Jednakże art. 6(3) oraz motywy 41 i 45 przewidują, że przedmiotowy obowiązek prawny musi być:

- obowiązkiem państwa członkowskiego lub przepisem prawa unijnego, któremu administrator danych podlega; oraz
- musi być *„jasny i precyzyjny”*, a jego nałożenie możliwe do przewidzenia dla osób, które temu obowiązkowi podlegają.

Preambuła jasno określa, że przedmiotowy „obowiązek prawny” nie musi mieć charakteru ustawowego (tzn. wystarczy prawo zwyczajowe, jeśli tylko spełnia wymóg „jasności i precyzyjności”). Obowiązek prawny może obejmować swoim zakresem różne czynności przetwarzania danych podejmowane przez administratora, zatem nie trzeba określać odrębnych obowiązków prawnych dla każdej czynności przetwarzania danych.

6(1)(d) – Konieczne w celu ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby, jeśli osoba, której dane dotyczą jest niezdolna do wyrażenia zgody

Motyw 46 sugeruje, że ta podstawa może mieć zastosowanie do przetwarzania danych, które jest konieczne dla celów humanitarnych (np. monitorowanie epidemii) lub w związku z przeciwdziałaniem skutkom kryzysów humanitarnych (np. interwencja po katastrofie). Punkt ten wskazuje, że w przypadkach, gdy przetwarzanie danych osobowych odbywa się w celu ochrony żywotnych interesów osoby innej, niż osoba, której dane dotyczą, na tę podstawę przetwarzania danych można się powoływać tylko wtedy, gdy nie ma innych podstaw prawnych.

6(1)(e) – Konieczne dla wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi

Art. 6(3) i Motyw 45 jasno określają, że ta podstawa ma zastosowanie wyłącznie w przypadku, gdy realizowane zadanie lub sprawowana władza publiczna administratora jest przewidziana w unijnym lub krajowym prawie, któremu podlega administrator danych.

6(1)(f) – Niezbędne do celów wynikających z prawnie uzasadnionych interesów

Na tę podstawę nie mogą się już powoływać organy publiczne przetwarzające dane osobowe w ramach wykonywania obowiązków publicznych; Motywy 47-50 dodatkowo precyzują, co można rozumieć pod pojęciem „prawnie uzasadnionego interesu” (więcej informacji znajduje się w części poświęconej prawnie uzasadnionym interesom).

Państwa członkowskie mogą wprowadzać szczegółowe przepisy stanowiące podstawę prawną zgodnie z art. 6(1)(c) i 6(1)(e) (przetwarzanie w związku z obowiązkiem prawnym lub wykonywaniem zadania w interesie publicznym lub w ramach sprawowania władzy publicznej) lub w innych, szczególnych sytuacjach związanych z przetwarzaniem danych (np. w związku z działalnością dziennikarską lub badawczą). Prawdopodobnie spowoduje to pewne rozbieżności w różnych państwach UE (więcej informacji na ten temat znajduje się w części poświęconej wyjątkom i warunkom szczególnym).

Dalsze przetwarzanie

RODO przewiduje także określone zasady (w art. 6(4)) dotyczące czynników, jakie administrator musi uwzględnić dokonując oceny tego, czy nowy cel przetwarzania danych jest zgodny z celami, dla których dane były pierwotnie zbierane. W przypadku, gdy takie przetwarzanie nie jest oparte na wyrażonej zgodzie, ani też na przepisach prawa UE lub państwa członkowskiego w zakresie kwestii określonych w art. 23 (przepisy ogólne dotyczące ograniczeń w zakresie ochrony bezpieczeństwa narodowego, prowadzenia postępowania przygotowawczego itd.), w celu ustalenia zgodności należy uwzględnić następujące czynniki:

- jakikolwiek związek pomiędzy pierwotnym celem a nowymi celami przetwarzania danych;
- kontekst, w którym zebrano dane osobowe (w szczególności relacje między osobami, których dane dotyczą, a administratorem);
- charakter danych (w szczególności fakt, czy stanowią one dane wrażliwe lub dane o wyrokach skazujących);
- ewentualne konsekwencje zamierzonego przetwarzania; oraz
- istnienie zabezpieczeń (w tym szyfrowania lub pseudonimizacji).

Motyw 50 wskazuje, że dalsze przetwarzanie dla celów archiwalnych w interesie publicznym, dla celów badań historycznych lub naukowych lub też w celach statystycznych, powinno być uznane za zgodne z prawem (więcej informacji na ten temat znajduje się w części poświęconej zgodzie i warunkom szczególnym).

Gdzie mogę to znaleźć?
Prawne podstawy przetwarzania
art. 6-10, motywy 40-50

Prawnie uzasadniony interes

Na pierwszy rzut oka

- Inaczej, niż w przypadku organów publicznych, dla przedsiębiorców kategoria *„prawnie uzasadnionego interesu”*, jako podstawa zgodnego z prawem przetwarzania, nie została w znacznym stopniu zmieniona przez przepisy RODO.
- Organy publiczne nie będą mogły powoływać się na *“prawnie uzasadniony interes”* w celu uzasadnienia przetwarzania danych w ramach pełnienia swojej funkcji.
- Administratorzy, którzy powołują się na *„prawnie uzasadniony interes”*, powinni zachować zapis oceny, którą w tym celu przeprowadzili, aby wykazać, iż uwzględnili i rozważyli kwestię praw i wolności osób, których dane dotyczą.
- Administratorzy powinni mieć świadomość, że do przetwarzania danych na podstawie prawnie uzasadnionego interesu zastosowanie znajduje prawo do sprzeciwu, które nie musi być realizowane jedynie w przypadku, gdy interes administratora ma nadrzędny charakter.

Co trzeba zrobić

- Należy upewnić się, że określili Państwo podstawy zgodnego z prawem przetwarzania danych, na których opiera się działalność Państwa organizacji, a także sprawdzić, czy te podstawy nadal będą ważne po wejściu w życie RODO (więcej informacji na ten temat znajduje się w części poświęconej przetwarzaniu i dalszemu przetwarzaniu).
- W przypadku, gdy Państwa organizacja jest organem publicznym, który aktualnie powołuje się na *„prawnie uzasadniony interes”* jako podstawę przetwarzania danych osobowych w związku z pełnieniem swojej funkcji, należy określić inną podstawę prawną dla przetwarzania danych (np. przetwarzanie danych jest konieczne w interesie publicznym lub w ramach sprawowania władzy publicznej)
- W przypadku powoływania się na *„prawnie uzasadniony interes”*, należy zapewnić, że sposób podejmowania decyzji w zakresie równoważenia interesów administratora danych (lub strony trzeciej) i praw osób, których dane dotyczą, jest dobrze udokumentowany, szczególnie w przypadku, gdy dotyczy dzieci. Należy także zapewnić, że osoby, których dane dotyczą, mają uzasadnione przesłanki by spodziewać się, że może dojść do przetwarzania ich danych w związku z prawnie uzasadnionym interesem administratora, lub strony trzeciej.
- W przypadku powoływania się na *“prawnie uzasadniony interes”* należy zapewnić, że kwestia ta jest uwzględniona w informacji, jaka musi zostać przekazana osobom, których dane dotyczą zgodnie z przepisami art. 13 i 14 (więcej informacji na ten temat znajduje się w części poświęconej informacjom dla osób, których dane dotyczą).

Komentarz

Art. 6(1) RODO określa, że przetwarzanie danych jest zgodne z prawem wyłącznie wtedy, gdy zastosowanie ma przynajmniej jeden z przepisów art. 6(1) (a)-(f).

Art. 6(1)(f) ma zastosowanie w przypadku, gdy:

«„przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem."»

Art. 6(1) w jasny sposób określa, że podpunkt (f) nie ma zastosowania do *„przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań."»*

Jest to generalnie powielenie odpowiedniego przepisu dyrektywy w sprawie ochrony danych, z tym że:

- dodana została potrzeba uwzględnienia interesów i praw dzieci (więcej informacji w części poświęconej dzieciom). W praktyce, dodanie tego elementu prawdopodobnie spowoduje nałożenie na administratorów wymogu zapewnienia, że wszelkie decyzje dotyczące przetwarzania danych dzieci na podstawie *„prawnie uzasadnionego interesu"* będą szczegółowo udokumentowane oraz, że przeprowadzona zostanie ocena skutków dla ochrony danych; oraz
- na *„prawnie uzasadniony interes"* nie mogą się już powoływać organy publiczne w odniesieniu do danych przetwarzanych przez nie podczas pełnienia swojej funkcji.

Co to jest prawnie uzasadniony interes?

Preambuła podaje przykłady przetwarzania danych, które może być niezbędne do celów wynikających z prawnie uzasadnionych interesów administratora. Powyższe obejmuje:

- Motyw 47: przetwarzanie dla potrzeb marketingu bezpośredniego lub w celu zapobiegania oszustwom;
- Motyw 48: przesyłanie danych osobowych w grupie przedsiębiorstw dla celów administracyjnych, w tym danych klientów i pracowników (uwaga: wymogi dot. przesyłania danych za granicę nadal mają zastosowanie - więcej informacji znajduje się w części poświęconej przesyłaniu danych osobowych);
- Motyw 49: przetwarzanie dla potrzeb zapewnienia bezpieczeństwa sieci i informacji, w tym w celu zapobiegania nieuprawnionemu dostępowi do sieci łączności elektronicznej, a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej; oraz
- Motyw 50: zgłaszanie możliwości popełnienia przestępstwa lub potencjalnych zagrożeń bezpieczeństwa publicznego właściwym organom.

Motyw 47 stanowi ponadto, że administratorzy danych powinni uwzględnić oczekiwania osób, których dane dotyczą, podczas dokonywania oceny tego, czy ich prawnie uzasadniony interes jest podrzędny w stosunku do interesów osób, których dane dotyczą. Interesy i podstawowe prawa osób, których dane dotyczą *„mogą być nadrzędne"* w stosunku do interesów administratora w przypadku, gdy osoby, których dane dotyczą *"nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania"*.

Prawnie uzasadniony interes musi zostać określony w informacjach dla osób których dane dotyczą

W przypadku powoływania się na "*prawnie uzasadniony interes*" w odniesieniu do określonych czynności przetwarzania danych, powyższe będzie trzeba określić w odpowiednich informacjach dla osób których dane dotyczą zgodnie z art. 13 (1)(d) i 14 (2)(b).

Szczególne i wzmocnione prawo do sprzeciwu

Osobom fizycznym przysługuje prawo do sprzeciwu wobec przetwarzania ich danych na podstawie uzasadnionego interesu. Od teraz to na administratorach danych spoczywa obowiązek wykazania, że ich interes ma nadrzędny charakter, aby uzasadnić konieczność dalszego przetwarzania danych. Może to prowadzić do wykonywania praw do ograniczenia przetwarzania lub usunięcia danych (więcej informacji znajduje się w części poświęconej prawu sprzeciwu).

Uwaga na kodeksy postępowania

Art. 40 wymaga, aby państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja Europejska zachęcały do tworzenia kodeksów postępowania w odniesieniu do szerokiego zakresu zagadnień, w tym pojęcia prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach. Członkowie zrzeszeń handlowych lub innych, podobnych organizacji sektorowych powinni zwrócić uwagę na powstawanie wspomnianych kodeksów postępowania, które mogą spowodować nałożenie określonych dodatkowych wymogów.

Przekazywanie danych do państw trzecich - nowa podstawa, ale istnieje małe prawdopodobieństwo, że kiedykolwiek znajdzie zastosowanie w praktyce.

Ostatnia wzmianka o prawnie uzasadnionych interesach znajduje się w art. 49(1), który stwierdza, że przekazywanie danych osobowych do państw trzecich może odbywać się na podstawie *„ważnych prawnie uzasadnionych interesów"* w przypadku, gdy przekazanie nie ma charakteru powtarzalnego, dotyczy tylko ograniczonej liczby osób, których dane dotyczą, i gdy administrator dokonał oceny i zapewnił odpowiedni stopień ochrony. Jednakże, na wspomnianą podstawę prawną można się powoływać wyłącznie w przypadku, gdy administrator nie może skorzystać z żadnej innej metody zapewnienia odpowiedniego stopnia ochrony, w tym za pomocą standardowych klauzul umownych, wiążących reguł korporacyjnych i wyjątków przewidzianych w art. 49(1)(a)-(f). Administrator danych musi w takim przypadku powiadomić organy nadzorcze o skorzystaniu z przedmiotowej podstawy prawnej dla celów przekazywania danych do państw trzecich. Wydaje się mało prawdopodobne, że organizacja będzie w stanie wykazać, że nie mogła powołać się na żadne inne podstawy przekazywania danych. (więcej informacji znajduje się w części poświęconej przekazywaniu danych osobowych do państw trzecich).

Gdzie mogę to znaleźć?

Prawnie uzasadniony interes
art. 6 ust. 1 lit. f), art. 13 ust. 1 lit. d), art. 14 ust. 2 lit. b), art. 49 ust. 1
motywy 47, 48, 49, 50

Zgoda

Na pierwszy rzut oka

- Zgoda podlega dodatkowym warunkom wynikającym z RODO.
- Dodatkowe wymogi obejmują zakaz powoływania się na *„wiązane”* zgody oraz oferowania usług w sposób uzależniony od zgody na przetwarzanie danych.
- Ponadto, na mocy nowych regulacji zgoda musi być wyrażona oddzielnie w stosunku do innych oświadczeń woli, a także jasno sformułowana i możliwa do cofnięcia w tak samo prosty sposób, w jaki została wyrażona.
- Szczególne zasady będą dotyczyć dzieci w odniesieniu do usług społeczeństwa informacyjnego.

Co trzeba zrobić

- Należy upewnić się, że nie mają Państwo wątpliwości co do podstaw zgodnego z prawem przetwarzania danych, na których opiera się działalność Państwa organizacji, a także sprawdzić, czy te podstawy nadal będą ważne po wejściu w życie RODO (więcej informacji na ten temat znajduje się w części poświęconej przetwarzaniu i dalszemu przetwarzaniu).
- Należy rozważyć, czy nowe zasady dotyczące przetwarzania danych dzieci w działalności internetowej będą Państwa dotyczyć, a jeśli tak, jakich krajowych zasad będą Państwo musieli przestrzegać w kontekście uzyskiwania zgody dzieci (więcej informacji w części poświęconej dzieciom).

Co trzeba zrobić

- W przypadku, gdy Państwa organizacja powołuje się na zgodę na przetwarzanie danych osobowych dla celów badań naukowych, sugerujemy rozważyć stworzenie osobom, których dane dotyczą, możliwości wyrażenia zgody tylko w odniesieniu do określonych obszarów badań lub części projektów badawczych.
- W przypadku, gdy zgoda stanowi podstawę przetwarzania danych, należy zapewnić że:
  - zgoda została wyrażona w sposób aktywny, oraz, że nie została wyrażona na zasadzie milczenia, niepodejmowania działań lub domyślnie zaznaczonych okienek;
  - zgoda na przetwarzanie danych jest łatwa do odróżnienia, jasna oraz nie jest „powiązana” z innymi pisemnymi porozumieniami lub oświadczeniami;
  - świadczenie usług nie jest uzależnione od wyrażenia zgody na przetwarzanie danych jeśli wyrażenie zgody nie jest niezbędne do umożliwienia świadczenia usługi;
  - osoby, których dane dotyczą są poinformowane o tym, że mają prawo wycofać zgodę w każdym czasie oraz, że nie będzie to miało wpływu na zgodność z prawem przetwarzania danych opartego na zgodzie w okresie przed jej wycofaniem;
  - istnieją proste sposoby wycofania zgody, w tym metody wykorzystujące te same kanały, za pomocą których zgoda została pierwotnie wyrażona;
  - osobne zgody zostały uzyskane dla odrębnych operacji przetwarzania; oraz
  - zgoda nie jest wykorzystywana jako podstawa prawna w przypadkach, gdy istnieje wyraźny brak równowagi pomiędzy osobą, której dane dotyczą, a administratorem (w szczególności w przypadku, gdy administratorem jest organ publiczny).

Komentarz

Zgoda - szersza definicja

Art. 4(11) RODO określa *„zgodę osoby, której dane dotyczą"* jako *„dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych."*

Wymóg, według którego zgoda musi być *„jednoznaczna"* nie stanowi zmiany w aspekcie praktycznym; art. 7(a) dyrektywy w sprawie ochrony danych stwierdza, że w przypadku, gdy zgoda stanowi podstawę prawną dla przetwarzania danych, musi ona być wyrażona w sposób *„jednoznaczny"*. Motyw 32 sugeruje, że może to polegać na:

"zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych (...) lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody."

Wyraźna zgoda jest nadal wymagana w celu uzasadnienia przetwarzania danych wrażliwych chyba, że zastosowanie mają inne podstawy prawne (więcej informacji w części poświęconej danym wrażliwym i przetwarzaniu zgodnie z prawem). Ponadto, gdy brak jest adekwatności lub innych warunków przetwarzania, wyraźna zgoda może być podstawą transferu danych poza obszar UE (więcej informacji w części poświęconej transferom danych) oraz służyć jako jedna z podstaw prawnych zautomatyzowanego podejmowania decyzji odnoszącego się do osoby fizycznej (więcej informacji w części poświęconej profilowaniu i zautomatyzowanemu podejmowaniu decyzji).

Warunki wyrażenia zgody - łatwość odróżnienia, możliwość wycofania i szczegółowość

Art. 7(1) RODO stanowi, że przypadku, gdy zgoda stanowi podstawę prawną dla przetwarzania danych, administratorzy powinni być w stanie wykazać, że zgoda na przetwarzanie danych została wyrażona przez osobę, której dane dotyczą. Pozostała część treści art. 7 skupia się na określeniu warunków, jakie zgoda musi spełnić, aby została uznana za ważną. Warunkami tymi są:

- Art. 7(2): Zgoda na przetwarzanie zawarta w pisemnym oświadczeniu przygotowanym przez administratora musi być możliwa do odróżnienia od innych kwestii zawartych w przedmiotowym oświadczeniu, a także w zrozumiałej i łatwo dostępnej formie oraz napisana jasnym i prostym językiem. Motyw 42 odwołuje się do dyrektywy w sprawie nieuczciwych warunków w umowach konsumenckich (Dyrektywa 93/13/EWG) jako inspiracji dla wspomnianych obowiązków. W praktyce zaistnieje wymóg, aby zgoda na przetwarzanie danych była łatwa do odróżnienia w obrębie umów i porozumień.

  Motyw 42 stanowi także, że zgoda jest uznawana za świadomą tylko wtedy, gdy osoba, której dane dotyczą, zdaje sobie sprawę (przynajmniej) z tożsamości administratora danych i celu przetwarzania;

- Art. 7(3): Osoby, których dane dotyczą, muszą mieć prawo do wycofania wyrażonej zgody w każdym czasie i z taką samą łatwością, z jaką zgoda została wyrażona. W praktyce, zgodnie z tym postanowieniem organizacje będą musiały umożliwić wycofanie zgody za pomocą tego samego kanału (np. strona internetowa, poczta elektroniczna, wiadomość tekstowa), jakim została wyrażona. Ponadto, RODO uwzględnia fakt, że wycofanie zgody nie powoduje, że dotychczasowe przetwarzanie danych staje się niezgodne z prawem, jednakże administrator jest zobowiązany poinformować o tym fakcie osoby, których dane dotyczą, zanim zgoda zostanie wyrażona; oraz

- Art. 7(4): W przypadku, gdy wykonanie umowy, w tym świadczenie usług, jest uzależnione od zgody na przetwarzanie danych osobowych, której wyrażenie nie jest niezbędne dla realizacji postanowień wspomnianej umowy, dobrowolność wyrażonej zgody może zostać zakwestionowana.

Motyw 43 wskazuje, że zgody nie uznaje się za wyrażoną dobrowolnie w przypadku, gdy:

- pomimo, że zgoda jest odpowiednia do aktualnych okoliczności, nie zapewniono możliwości wyrażenia zgody w odniesieniu do odrębnych operacji przetwarzania danych; lub

- *„gdy wykonanie umowy, w tym świadczenie usługi, jest uzależnione od zgody, pomimo faktu, że przedmiotowa zgoda nie jest konieczna dla świadczenia wspomnianej usługi"*

W rezultacie, świadczenie usługi nie może być uzależnione od wyrażenia przez osobę, której dane dotyczą, zgody na przetwarzanie jej danych osobowych, jeśli nie jest to niezbędne do świadczenia usługi.

Dzieci i działalność badawcza

Szczególnym warunkom podlega ważność zgody wyrażonej przez dzieci w odniesieniu do usługi społeczeństwa informacyjnego, w którym to kontekście pojawia się wymóg uzyskania i zweryfikowania zgody rodzica poniżej pewnego limitu wiekowego (więcej informacji na ten temat znajduje się w części poświęconej danym dzieci).

Motyw 33 RODO dotyczy zgody uzyskanej w odniesieniu do przetwarzania danych dla celów badań naukowych. Postanowienie to stanowi, że *„w momencie zbierania danych często nie da się w pełni zidentyfikować celu przetwarzania danych osobowych na potrzeby badań naukowych"*, a także, iż:

- osoby, których dane dotyczą powinny mieć możliwość wyrażenia zgody na niektóre obszary badań naukowych, o ile są one zgodne z *„uznanymi normami etycznymi"* w zakresie takich badań; oraz

- osoby, których dane dotyczą powinny mieć możliwość wyrażenia zgody tylko na *„niektóre obszary badań lub elementy projektów badawczych, o ile umożliwia to zamierzony cel"*.

Język, w którym zgoda została sformułowana

RODO wymaga, aby zgoda była zrozumiała, świadoma, jednoznaczna etc. Zgoda nie będzie spełniać tych warunków jeżeli będzie sporządzona w języku, którym osoba fizyczna nie włada. Jest wysoce prawdopodobne, że zasady kierowania swoich działań do osób fizycznych w związku z zakresem terytorialnym RODO znajdą zastosowanie również wtedy, gdy administratorzy danych będą ustalać języki UE, w których powinna zostać sformułowana zgoda. Jeśli organizacja kieruje swoje działania do danej jurysdykcji, wydaje się wskazane przetłumaczenie zgody na język obowiązujący w tej jurysdykcji. Jednakże, odwrotna interpretacja nie została wykluczona przez RODO, tj. brak kierowania działań do danej jurysdykcji może nie wykluczać wymogu pozyskania zgody w języku tej jurysdykcji.

Gdzie mogę to znaleźć?

art. 4 pkt 11), art. 6 ust. 1 lit. a), art. 7 i 8, art. 9 ust. 2 lit. a)
motywy 32, 33, 42 oraz 43

Dzieci

Na pierwszy rzut oka

- W tekście RODO obecnych jest kilka przepisów dotyczących wyłącznie dzieci, w szczególności w odniesieniu do podstaw przetwarzania i informacji dla osób których dane dotyczą.
- Dzieci są określane jako osoby szczególnie podatne na zagrożenia i w związku z tym wymagające „*szczególnej opieki*".
- Przetwarzanie danych odnoszących się do dzieci jest uznawane za obarczone pewnym ryzykiem, i w związku z tym dalsze ograniczenia mogą zostać wprowadzone w rezultacie opracowywania kodeksów postępowania.
- RODO nie określa wieku, w którym osoba jest uznawana za dziecko.
- W przypadku świadczenia usług w internecie na rzecz dzieci, i gdy zgoda na przetwarzanie danych stanowi podstawę prawną przetwarzania danych dziecka, zgoda musi zostać wydana lub potwierdzona przez osobę sprawującą władzę rodzicielską nad dzieckiem. Wymóg ten dotyczy dzieci poniżej 16 roku życia (chyba, że dane państwo członkowskie obniżyło próg wieku, przy czym nie może on być niższy, niż 13 lat).

Co trzeba zrobić

- ☐ Należy rozważyć, czy nowe zasady dotyczące danych dzieci będą Państwa dotyczyć.
- ☐ W przypadku, gdy Państwa organizacja oferuje usługi w ramach społeczeństwa informacyjnego świadczone na rzecz dzieci, należy ocenić, które krajowe przepisy będą miały zastosowanie, oraz zapewnić, że wdrożone zostały odpowiednie mechanizmy uzyskiwania zgody rodzicielskiej w tym w zakresie weryfikacji wyrażonej zgody.
- ☐ Należy mieć na uwadze lokalnie obowiązujące prawo w zakresie przetwarzania danych poza Internetem w zakresie danych osobowych dzieci.
- ☐ W przypadku, gdy usługi są oferowane bezpośrednio dziecku, należy zapewnić, że informacje dla osób których dane dotyczą są napisane jasnym językiem i będą dla dziecka zrozumiałe.
- ☐ Należy zapewnić, że przy powoływaniu się na „*prawnie uzasadniony interes*" jako podstawę przetwarzania danych dzieci, dokonano skrupulatnej i dobrze udokumentowanej oceny tego, czy interesy dziecka nie są nadrzędne w stosunku do interesów Państwa organizacji.
- ☐ Należy zwrócić uwagę na ewentualne kodeksy postępowania, które mogą mieć wpływ na stowarzyszenia i grupy, do których Państwa organizacja należy.

Komentarz

Waga kwestii ochrony dzieci jest wspomniana kilkukrotnie w treści RODO. W praktyce, nowy tekst nie zapewnia harmonizacji, a znaczne ograniczenia prawdopodobnie powstaną w następstwie istniejących lub nowych regulacji krajowych lub kodeksów postępowania (więcej informacji znajduje się w części poświęconej kodeksom postępowania i certyfikacji).

Zgoda rodzica

Dyrektywa w sprawie ochrony danych nie zawiera żadnych szczególnych ograniczeń w zakresie przetwarzania danych dzieci, a zasady dotyczące możliwości wyrażania przez dzieci zgody mają swe źródło w przepisach prawa krajowego. RODO nie zapewnia w tym zakresie harmonizacji. Najważniejszym postanowieniem dotyczącym dzieci jest art. 8, który wymaga wyrażenia zgody przez rodzica w przypadku usług w ramach społeczeństwa informacyjnego oferowanych bezpośrednio dziecku w wieku do 16 lat - przy czym próg ten może być obniżony do 13 lat przez państwo członkowskie i ma zastosowanie wyłącznie w przypadku przetwarzania danych na podstawie zgody wyrażonej przez dziecko. Nie wiadomo czy powyższy obowiązek uzyskania zgody będzie miał zastosowanie, jeżeli zgoda zostanie pobrana nieintencjonalnie z wykorzystaniem internetu. Wstępne wytyczne organu nadzorczego w Wielkiej Brytanii (ang. *Information Commissioner's Office*) zakładają, że uzyskanie zgody dziecka będzie konieczne, jeżeli usługa społeczeństwa informacyjnego będzie skierowana do dzieci.

Administrator podlega także, na mocy art. 8(2) RODO, wymogowi podjęcia *„rozsądnych starań"* w celu zweryfikowania, czy zgoda została wyrażona lub potwierdzona przez osobę posiadającą władzę rodzicielską uwzględniając dostępną technologię.

Ma to wpływ tylko na niektóre kategorie danych internetowych. Dane spoza internetu nadal będą podlegać zasadom obowiązującym w danym państwie członkowskim w zakresie zdolności do wyrażania zgody. Art. 8(1) także należy uwzględnić jako przepis, który wpływa na ogólne przepisy prawa zobowiązań poszczególnych państw członkowskich w zakresie ważności oraz zawierania lub skutków umowy z dzieckiem. Organizacje nadal będą musiały uwzględnić lokalne prawo w tym obszarze.

Informacje przekazywane dzieciom muszą być napisane odpowiednim dla nich językiem.

Art. 12 RODO stanowi, że obowiązki w zakresie zapewnienia, że informacje przekazywane osobom, których dane dotyczą, muszą być zwięzłe, przejrzyste i sformułowane prostym językiem, należy realizować „w szczególności gdy informacje są kierowane do dziecka". Zgodnie z motywem 58:

„Zważywszy że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty – gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć".

Pojęcie *„dziecko"* nie zostało zdefiniowane w RODO. Administratorzy powinni zatem być przygotowani na sprostanie tym wymogom w informacjach kierowanych bezpośrednio do nastolatków i młodzieży.

Przepisy końcowe - infolinie, kodeksy postępowania i praca na rzecz organów nadzorczych

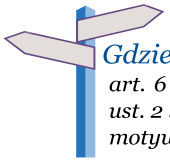
Art. 6(1)(f) RODO przewiduje, że prawa i wolności osoby, której dane dotyczą, mogą być nadrzędne w stosunku do interesów administratora lub osoby trzeciej „w szczególności", jeśli osoba, której dane dotyczą, jest dzieckiem. Administratorzy powinni zapewnić prowadzenie dokumentacji wykazującej, że sporne interesy zostały należycie rozważone w przypadku, gdy prawnie uzasadniony interes jest podstawą prawną przetwarzania danych dzieci.

Motyw 38 przewiduje, że korzystanie z danych dzieci w celach marketingowych, lub dla celów profilowania w związku ze świadczeniem usług na rzecz dzieci, to obszary wymagające szczególnej ochrony na mocy przepisów RODO. Motyw ten stanowi także, że zgoda rodzicielska nie powinna być wymagana przy usługach profilaktyki lub doradztwa oferowanych bezpośrednio dziecku, jednakże ta sugestia nie znajduje odzwierciedlenia wprost w treści RODO.

Motyw 75 stwierdza, że dzieci są „osobami wymagającymi szczególnej opieki" i że przetwarzanie danych dzieci jest czynnością, która może sprowadzić ryzyko „o różnym prawdopodobieństwie i wadze zagrożeń".

Art. 40 wymaga, aby państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja Europejska zachęcały do tworzenia kodeksów postępowania, między innymi w obszarze ochrony dzieci, w tym w zakresie sposobu w jaki pozyskuje się zgodę od osoby sprawującej władzę rodzicielską. Organizacje, które przetwarzają dane osobowe odnoszące się do dzieci powinny zwrócić uwagę na powstawanie takich kodeksów, które mogą spowodować nałożenie określonych dodatkowych wymogów.

Wreszcie, organy nadzorcze, realizując zadanie wzmacniania świadomości publicznej i upowszechnia w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych, zgodnie z obowiązkiem nałożonym na nie przez art. 57(1)(b), muszą zwrócić „szczególną uwagę" na działania, które są skierowane do dzieci.



Gdzie mogę to znaleźć?

art. 6 ust.1 lit. f), art. 8, art. 12 ust. 1, art. 40 ust. 2 lit. g), art. 57 ust. 1 lit. b)
motyw 38, 58, 75

Dane wrażliwe i przetwarzanie zgodnie z prawem

Na pierwszy rzut oka

- *„Szczególne kategorie danych osobowych”* (dane wrażliwe) obecnie obejmują konkretnie *„dane genetyczne”* i *„dane biometryczne”* jeśli są one przetwarzane *„w celu jednoznacznego zidentyfikowania osoby”*.
- Podstawy do przetwarzania danych wrażliwych na mocy RODO są generalnie powieleniem podstaw przewidzianych w dyrektywie w sprawie ochrony danych, istnieją jednak szersze podstawy w obszarze zdrowia i zarządzania opieką zdrowotną.
- Państwa członkowskie otrzymały także duże możliwości ustanawiania nowych warunków (w tym także ograniczeń) w zakresie przetwarzania danych genetycznych, biometrycznych oraz informacji na temat stanu zdrowia.

Co trzeba zrobić

☐	Należy upewnić się, że rozumieją Państwo podstawy przetwarzania danych, na których opiera się działalność Państwa organizacji w zakresie przetwarzania danych wrażliwych, a także sprawdzić, czy te podstawy nadal będą ważne po wejściu w życie RODO.
☐	W przypadku, gdy wyżej wspomnianą podstawę stanowi zgoda, należy zapewnić, że wyrażona zgoda spełnia nowe wymogi w zakresie jej uzyskiwania (więcej informacji znajduje się w części poświęconej wyrażaniu zgody);
☐	Należy rozważyć, czy nowe zasady dotyczące danych dzieci będą Państwa dotyczyć, a jeśli tak, jakich krajowych zasad będą Państwo musieli przestrzegać Przy uzyskiwaniu zgody (więcej informacji znajduje się w części poświęconej dzieciom); a także
☐	W przypadku, gdy dysponują Państwo dużymi ilościami danych genetycznych, biometrycznych oraz informacji na temat stanu zdrowia, należy bacznie obserwować rozwój krajowej legislacji, ponieważ państwa członkowskie posiadają duże możliwości w zakresie nakładania nowych warunków, w tym także ograniczeń, w stosunku do podstaw prawnych przewidzianych w treści RODO.

Komentarz

Art. 9(2) określa okoliczności, w których przetwarzanie danych wrażliwych jest dopuszczalne. Następujące kategorie danych są uznawane za „*wrażliwe*", zgodnie z treścią art. 9(1):

- pochodzenie rasowe lub etniczne;
- poglądy polityczne;
- przekonania religijne lub światopoglądowe;
- przynależność do związków zawodowych;
- dane dotyczące zdrowia, seksualności i orientacji seksualnej;
- dane genetyczne (*nowe*); oraz
- dane biometryczne, jeżeli są one przetwarzane w celu zidentyfikowania osoby (nowe).

Należy zwrócić uwagę, że Motyw 51 sugeruje, że przetwarzanie danych w postaci fotografii nie jest automatycznie uznawane za przetwarzanie danych wrażliwych (jak to miało miejsce dotychczas w niektórych państwach członkowskich); fotografie są objęte przedmiotowym ograniczeniem wyłącznie w zakresie, w którym pozwalają na identyfikację lub poświadczenie tożsamości osoby fizycznej, jako informacja o charakterze biometrycznym (np. jeśli jest częścią elektronicznego paszportu).

Podstawy prawne przetwarzania danych wrażliwych zasadniczo powielają odpowiednie przepisy zawarte w dyrektywie w sprawie ochrony danych. Powyższe obejmują:

9(2)(a) - Wyraźna zgoda osoby, której dane dotyczą, chyba że powoływanie się na zgodę jest zabronione na mocy prawa danego państwa członkowskiego

Bez zmian, jednak należy uwzględnić nowe warunki dla wyrażania zgody (więcej informacji znajduje się w części poświęconej wyrażaniu zgody).

9(2)(b) - Konieczne Niezbędne do wypełnienia obowiązków wynikających z prawa pracy, zabezpieczenia społecznego i ochrony socjalnej lub porozumienia zbiorowego

Jest to w pewnym sensie rozszerzenie sformułowań zawartych w dyrektywie w sprawie ochrony danych w tym zakresie, że pojawia się wyraźne odniesienie do zgodności ze zbiorowymi układami pracy i zobowiązaniami wynikającymi z ubezpieczeń społecznych.

9(2)(c) - Niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, a która jest fizycznie lub prawnie niezdolna do wyrażenia zgody

Jest to generalnie powielenie odpowiedniego przepisu dyrektywy w sprawie ochrony danych.

9(2)(d) – Przetwarzanie przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych pod warunkiem, że przetwarzanie dotyczy wyłącznie do aktualnych lub byłych członków tego podmiotu (lub osób, z którymi podmiot ma stały kontakt celów związku z jego celami), a także pod warunkiem, że nie ujawnia się danych stronom trzecim bez uprzedniej zgody

Jest to generalnie powielenie odpowiedniego przepisu dyrektywy w sprawie ochrony danych.

9(2)(e) – Przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą

Jest to generalnie powielenie odpowiedniego przepisu dyrektywy w sprawie ochrony danych.

9(2)(f) Niezbędne do ustalenia, dochodzenia lub obrony roszczeń, lub w ramach sprawowania wymiaru sprawiedliwości przez sądy

Przetwarzanie danych przez sądy w ramach sprawowania wymiaru sprawiedliwości zostało dodane do odpowiedniego przepisu dyrektywy w sprawie ochrony danych.

9(2) (g) - Niezbędne ze względu na ważny interes publiczny na podstawie prawa UE lub prawa państwa członkowskiego, które jest proporcjonalne do celów i które zapewnia odpowiednie środki zabezpieczające

Pozwala to państwom członkowskim na rozszerzenie, na podstawie przepisów prawa, zakresu przypadków, w których przetwarzanie danych wrażliwych jest dopuszczalne w interesie publicznym.

99(2)(h) – Niezbędne dla celów profilaktyki zdrowotnej lub medycyny pracy, w celu dokonania oceny zdolności do pracy pracownika, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia, lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa UE lub prawa państwa członkowskiego, lub też na podstawie umowy zawartej z pracownikiem służby zdrowia

ORAZ

9(2)(i) - Niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, w tym ochrony przed poważnymi transgranicznymi zagrożeniami zdrowotnymi, lub zapewniania wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych

Powyższe dwa przepisy zostały dodane do odpowiedniego przepisu dyrektywy w sprawie ochrony danych w celu wyeliminowania luk w jej treści poprzez, na przykład, zapewnienie formalnego, prawnego uzasadnienia dla wykorzystywania danych o stanie zdrowia w celach regulacyjnych w sektorach opieki zdrowotnej i farmaceutycznym, a także poprzez umożliwienie dzielenia się danymi o stanie zdrowia z dostawcami usług opieki zdrowotnej.

Oba warunki wymagają wprowadzenia zobowiązań do ochrony poufności za pomocą odpowiednich mechanizmów zabezpieczających..

9(2)(j) - Niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych zgodnie z art. 89(1)

Jest to nowy przepis dotyczący przetwarzania danych wrażliwych dla celów archiwalnych, a także dla celów badań i statystyki, z zastrzeżeniem zgodności z odpowiednimi wymogami w zakresie bezpieczeństwa, w tym mechanizmami zabezpieczającymi mającymi za zadanie zapewnić przestrzeganie zasady minimalizacji danych (więcej informacji znajduje się w części poświęconej wyjątkom i warunkom szczególnym).

Dane genetyczne, biometryczne oraz informacje na temat stanu zdrowia

Państwa członkowskie mają prawo, na mocy art. 9(4) RODO, do utrzymywania lub wprowadzania dodatkowych warunków (w tym ograniczeń) w zakresie danych genetycznych, biometrycznych oraz informacji na temat stanu zdrowia. W związku z tym, istniejące różnice w podejściu do tych kwestii prawdopodobnie utrzymają się, a nawet możliwe jest pojawienie się dalszych rozbieżności. Podmioty przetwarzające te kategorie danych powinny nadal bacznie obserwować rozwój właściwych przepisów prawa krajowego, a także rozważyć potrzebę wspierania działań lobbingowych w tym obszarze.

Wyroki skazujące i naruszenia prawa

Dane dotyczące wyroków skazujących i naruszeń prawa nie należą do kategorii „danych wrażliwych" w myśl RODO. Powyższe nie stanowi jednak zmiany względem dyrektywy w sprawie ochrony danych, na mocy której dane tego rodzaju również nie były traktowane jako dane wrażliwe. Nie zmienia to jednak faktu, że na podstawie polskiej ustawy o ochronie danych osobowych, dane dotyczące postępowań karnych i wyroków skazujących są uznawane za dane wrażliwe.

Zasady wynikające z RODO w odniesieniu do danych dotyczących wyroków skazujących i naruszeń prawa odzwierciedlają zasady stosowane na gruncie dyrektywy w sprawie ochrony danych. Art. 10 stanowi, że tego typu dane mogą być przetwarzane wyłącznie pod nadzorem władz publicznych lub w przypadku, gdy takie przetwarzanie jest przewidziane w unijnym lub krajowym prawie, które zapewniają odpowiednie zabezpieczenia. Powyższy przepis prawdopodobnie doprowadzi do dalszych rozbieżności w przepisach krajowych w tym obszarze.

Gdzie mogę to znaleźć?
art. 9
motyw 51-56

Informacje dla osób, których dane dotyczą

Na pierwszy rzut oka

- Administratorzy muszą dostarczyć odpowiednie informacje dla osób których dane dotyczą w celu zapewnienia przejrzystości przetwarzania.
- Należy dostarczyć szczegółowych informacji, a ponadto istnieje ogólny obowiązek zapewnienia przejrzystości.
- Dostarczenie większości wspomnianych informacji dodatkowych nie powinno być trudne, jednak kłopotliwe może okazać się poinformowanie o okresie, przez który dane osobowe będą przechowywane.
- Nacisk położono na jasność i zwięzłość informacji dla osób, których dane dotyczą

Co trzeba zrobić

- Należy sprawdzić istniejące informacje dla osób, których dane dotyczą i w razie potrzeby dokonać zmian i uaktualnień.
- W przypadku danych, które są zbierane w sposób pośredni, należy zapewnić, aby przekazywanie informacji następowało w odpowiednim terminie.
- Zalecamy współpracę z podmiotami, które mogą zbierać informacje w imieniu Państwa organizacji tak, aby przenieść na te podmioty odpowiedzialność za przegląd, uaktualnianie i zatwierdzanie informacji.

Komentarz

Zasada *„rzetelnego i przejrzystego”* przetwarzania oznacza, że administrator jest zobowiązany dostarczyć osobom informacje na temat przetwarzania ich danych chyba, że wspomniane osoby już posiadają przedmiotowe informacje. Informacje, jakich należy dostarczyć, są wyszczególnione w treści RODO, a ich wykaz znajduje się poniżej. Administrator może także być zobowiązany do dostarczenia dodatkowych informacji, jeżeli, w zależności od kontekstu i okoliczności, będzie to konieczne w celu zapewnienia rzetelności i przejrzystości przetwarzania.

Informacje muszą być dostarczone w formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej, a także muszą być sformułowane prostym językiem (w szczególności jeśli osobami, których dane dotyczą, są dzieci).

O czym administrator musi poinformować osobę fizyczną?

RODO wymaga przekazania większego zakresu informacji, niż przepisy dyrektywy w sprawie ochrony danych. Jednakże, wiele spośród dodatkowych informacji jest już wymagane na gruncie prawa krajowego niektórych państw członkowskich. Informacje, które nie są określone w dyrektywie w sprawie ochrony danych, zostały podane kursywą.

- Tożsamość i dane kontaktowe administratora (lub jego przedstawiciela, jeśli administrator nie ma jednostki organizacyjnej w UE); *dane kontaktowe inspektora ochrony danych.*
- Cel przetwarzania *i podstawa prawna przetwarzania - w tym także prawnie uzasadniony interes realizowany przez administratora (lub stronę trzecią) jeśli stanowi to podstawę prawną przetwarzania.*
- Informacje o odbiorcach danych osobowych lub o kategoriach odbiorców.
- Szczegółowe informacje na temat przekazywania danych poza terytorium UE:
  - *w tym informacje na temat sposobów ochrony danych (np. odbiorca znajduje się w odpowiednim państwie, wdrożone zostały wiążące reguły korporacyjne itd.) oraz*
  - *informacje na temat tego, w jaki sposób osoba fizyczna może otrzymać kopię wiążących reguł korporacyjnych lub innych zabezpieczeń, względnie gdzie informacje te są dostępne.*
- *Okres przechowywania danych - jeśli nie jest to możliwe, informacja na temat kryteriów jego ustalania.*
- Informacja o tym, że osoba fizyczna ma prawo do dostępu i *przenoszenia danych, a także do ich sprostowania, usuwania lub ograniczania przetwarzania, lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także, w przypadku, gdy przetwarzanie odbywa się na podstawie wyrażonej zgody, do wycofania zgody na przetwarzanie danych.*
- *Informacja o tym, że osoba fizyczna ma prawo złożyć skargę do organu nadzorczego.*
- *Informacja o tym, czy istnieje ustawowy lub umowny obowiązek dostarczenia informacji, a także konsekwencje niedostarczenia wspomnianych informacji.*
- Informacja o tym, czy przewidywane jest zautomatyzowane podejmowanie decyzji - wraz z informacją na temat zasad ich podejmowania oraz znaczenia i konsekwencji takiego przetwarzania dla osoby, której dane dotyczą.

Kiedy administrator musi dostarczyć wspomnianych informacji?

Administrator otrzymuje informację bezpośrednio od danej osoby fizycznej

- W momencie zbierania danych.

Administrator musi także poinformować osoby fizyczne o tym jakie informacje są obowiązkowe i jakie są konsekwencje ich nieprzekazania.

Administrator nie otrzymuje informacji bezpośrednio

- W uzasadnionym terminie po zebraniu danych (nie dłużej, niż jeden miesiąc); lub
- Jeśli dane są wykorzystywane do komunikowania się z daną osobą, najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
- Jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

Administrator musi także poinformować osoby fizyczne o kategoriach i źródłach informacji, w tym w przypadku, gdy informacje te pochodzą ze źródeł publicznie dostępnych.

- Administrator nie musi dostarczać tych informacji osobie fizycznej jeśli jest to niemożliwe, lub wymagało nieproporcjonalnie dużego wysiłku. W takim przypadku należy podjąć odpowiednie działania w celu ochrony interesów osób fizycznych oraz publicznie udostępnić odpowiednie informacje.

Nie ma potrzeby przekazywania indywidualnych informacji:

- w przypadku, gdy istnieje krajowy lub unijny obowiązek po stronie administratora danych w zakresie zbierania/ujawniania informacji; lub
- w przypadku, gdy dana informacja musi zostać zachowana w tajemnicy ze względu na zobowiązania zawodowe lub zobowiązania w zakresie zachowania tajemnicy, podlegające przepisom prawa UE lub prawa danego państwa członkowskiego.

W przypadku, gdy administrator dokonuje później przetwarzania danych osobowych dla nowego celu, który nie jest objęty zakresem pierwotnej informacji, administrator jest zobowiązany przekazać nową informację dotyczącą nowych czynności przetwarzania danych.

Dostarczanie wszystkich wyżej opisanych informacji jest trudne do pogodzenia z wymogiem zwięzłości i jasności, zawartym w RODO. Aby pomóc w realizacji tego obowiązku, przewidziano możliwość dla Komisji do wprowadzenia standardowych znaków graficznych za pomocą aktów delegowanych. Gdyby znaki te zostały wprowadzone, należałoby je prezentować osobom fizycznym.

Gdzie mogę to znaleźć?
art. 12-14
motywy 58, 60, 61 i 62

Prawo do dostępu, sprostowania i przenoszenia danych

Na pierwszy rzut oka

- Administrator danych osobowych musi, na żądanie:
  - potwierdzić, że przetwarza dane osoby fizycznej zgłaszającej zapytanie;
  - dostarczyć osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu (w wielu przypadkach w powszechnie stosowanym formacie elektronicznym); oraz
  - dostarczyć dodatkowe, szczegółowe materiały wyjaśniające.
- Osoby, których dane dotyczą, mogą zażądać swoich danych osobowych lub zażądać przeniesienia danych do nowego dostawcy w formie nadającej się do odczytu maszynowego w przypadku, gdy przedmiotowe dane: 1) były dostarczone administratorowi przez osobę, której dane dotyczą; 2) są przetwarzane w sposób zautomatyzowany; oraz 3) są przetwarzane na podstawie zgody lub w ramach realizacji umowy.
- Wyżej wspomniane żądanie musi zostać spełnione w terminie jednego miesiąca (w niektórych przypadkach możliwe jest przedłużenie tego okresu). Zamiar odstąpienia od realizacji żądania należy przedmiotowej osobie wyjaśnić.
- Prawo dostępu ma na celu umożliwienie osobom weryfikacji zgodności z prawem przetwarzania, a prawo do otrzymania kopii danych nie powinno negatywnie wpływać na prawa innych osób.

Co trzeba zrobić

☐	Należy dokonać przeglądu procesów, procedur i programów szkoleń dla pracowników mających kontakt z klientem, aby potwierdzić, że są one wystarczające do sprostania zasadom dotyczącym dostępu i przenoszenia danych przewidzianym w RODO.
☐	Należy opracować wzory odpowiedzi aby zawczasu zapewnić, że wszystkie elementy informacji dodatkowych zostały uwzględnione.
☐	Należy ocenić zdolność Państwa organizacji do dostarczenia danych w zgodności z wymogami co do formatów plików przewidzianych w RODO. Być może konieczne będzie opracowanie określonych formatów plików w celu sprostania żądaniom dostępu do danych.
☐	W przypadku, gdy prawo do przenoszenia danych ma zastosowanie, należy rozważyć, czy dane (i powiązane metadane) można łatwo wyeksportować w ustrukturyzowanym, nadającym się do odczytu maszynowego (i, w miarę możliwości, interoperacyjnym) formacie. Należy też śledzić inicjatywy branżowe, które mogą stworzyć formaty interoperacyjne.
☐	Należy rozważyć uruchomienie portalu dostępu dla osób, których dane dotyczą, aby umożliwić im korzystanie z prawa dostępu do danych w sposób bezpośredni.

Prawo do informacji i dostępu

Osobie fizycznej przysługują następujące prawa względem administratora danych:

- prawo do otrzymania potwierdzenia przetwarzania danych osobowych danej osoby fizycznej;
- prawo do dostępu do danych (np. w celu sporządzenia kopii) oraz
- prawo do otrzymania informacji dodatkowych na temat przetwarzania

Podobnie, jak w przypadku wszystkich innych praw osób, których dane dotyczą, administrator musi wykonać ciążący na nim obowiązek „*bez zbędnej zwłoki*" i „*najpóźniej w terminie miesiąca*", przy czym są pewne możliwości wydłużenia tego terminu.

Administrator musi także dołożyć uzasadnionych starań w celu potwierdzenia tożsamości osoby składającej żądanie - nie powinien jednak utrzymywać ani zbierać danych tylko w celu realizacji żądań o dostęp do danych ze strony osób, których dane dotyczą. Poniższe punkty dotyczą w szczególności usług świadczonych w internecie.

Prawo do dostępu do danych

Administrator jest zobowiązany do dostarczenia „*kopii danych osobowych podlegających przetwarzaniu*". Obowiązek ten nie podlega opłatom (co stanowi zmianę dla administratorów w Wielkiej Brytanii), jednakże administrator danych może naliczyć uzasadnioną opłatę administracyjną w przypadku, gdy pojawią się żądania udostępnienia dodatkowych kopii.

W przypadku, gdy żądanie zostanie złożone w formie elektronicznej, żądanych informacji należy dostarczyć w odpowiednim formacie elektronicznym (chyba, że osoba, której dane dotyczą, wskaże inaczej). Może to powodować ponoszenie kosztów przez administratorów, którzy wykorzystują specjalne formaty danych, lub którzy prowadzą archiwa w formie papierowej.

Motyw 63 sugeruje, że w miarę możliwości administrator może stworzyć bezpieczny system, który pozwala osobom, których dane dotyczą, na dostęp do ich danych osobowych. Wydaje się, że to rozwiązanie jest sugestią, nie zaś wymogiem.

Informacje dodatkowe

Administrator danych jest ponadto zobowiązany do dostarczenia następujących informacji (pozycje pisane kursywą nie są obecnie wymagane na mocy przepisów dyrektywy w sprawie ochrony danych, są jednak wymagane na mocy prawa niektórych państw członkowskich w ramach transpozycji dyrektywy w sprawie ochrony danych):

- cele przetwarzania;
- kategorie przetwarzanych danych;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców (*w szczególności informacje na temat ujawniania danych odbiorcom z innych państw lub międzynarodowych organizacji* (organizacji ukonstytuowanych na mocy prawa publicznego międzynarodowego lub utworzonych na mocy umów pomiędzy państwami));
- *przewidywany okres przechowywania, lub, jeśli nie jest to możliwe, informacja na temat kryteriów jego ustalania;*
- *prawo przysługujące osobom do sprostowania i usuwania danych, a także ograniczania przetwarzania oraz zgłaszania sprzeciwu i wnoszenia skarg do organów nadzorczych;*
- *informacje na temat źródła danych (jeśli nie są zbierane od osoby, której te dane dotyczą)*; oraz
- informacje na temat zautomatyzowanego podejmowania decyzji (np. decyzji podejmowanych wyłącznie w sposób zautomatyzowany, które wywołują wobec osoby skutki prawne lub w podobny sposób istotnie na nią wpływają, a także na temat zautomatyzowanego podejmowania decyzji odnośnie do danych wrażliwych) - wraz z informacją na temat wykorzystywanych w tym celu zasad oraz *znaczenia i przewidywanych skutków przetwarzania dla osoby, której dane dotyczą.*

Jeżeli administrator nie zamierza spełnić żądania, musi jednocześnie podać przyczyny takiej decyzji.

Odstępstwa

Przepisy RODO przewidują możliwość, iż dostęp osób, których dane dotyczą, może mieć niekorzystny wpływ na inne osoby i w związku z tym rozporządzenie zawiera przepis, na mocy którego prawo do otrzymania kopii danych jest uwarunkowane brakiem wyżej wspomnianego negatywnego wpływu. Motyw 63 stanowi, że warunek ten obejmuje swoim zakresem ochronę własności intelektualnej i tajemnicy handlowej (np. jeśli ujawnienie zasad zautomatyzowanego podejmowania decyzji oznaczałoby jednoczesne ujawnienie wyżej wspomnianych poufnych informacji). Jednakże przedmiotowy przepis stwierdza także, że administrator nie może odmówić dostarczenia wszystkich informacji z powodu tego, że udzielenie dostępu do danych może doprowadzić do naruszenia innych praw.

Motyw 63 zawiera ponadto dwa inne, użyteczne ograniczenia:

- w przypadku, gdy administrator dysponuje znaczną ilością danych, może zwrócić się do osoby, której dane dotyczą, o sprecyzowanie danych lub czynności przetwarzania, których dotyczy żądanie (jednakże motyw ten nie stwierdza, że istnieje jakiekolwiek odstępstwo wynikające z dużej ilości przechowywanych danych: ograniczenie ma najwyraźniej więcej wspólnego z charakterem żądania, niż zakresem czasu i pracy po stronie administratora – chociaż oba pojęcia mogą, rzecz jasna, być ze sobą wzajemnie powiązane);
- prawo osoby, której dane dotyczą, służy temu, by „*mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem*". Potwierdzają to komentarze sformułowane przez TSUE w sprawie *YS v Minister voor Immigratie, Integratie en Asiel* (sprawa C-141/12), według których cel uzyskania dostępu przez osobę, której dane dotyczą, polega na umożliwieniu osobie fizycznej potwierdzenia prawidłowości danych i zweryfikowania zgodności z prawem przetwarzania danych, a także umożliwienia osobom korzystania z przysługujących im praw do poprawiania danych i zgłaszania, w razie potrzeby, sprzeciwu. Innymi słowy, cel jest związany z prawami osoby fizycznej wynikającymi z przepisów o ochronie danych: żądania zgłoszone z innych powodów niezwiązanych z ochroną danych, mogą potencjalnie zostać odrzucone.

Prawo do sprostowania

Osoby fizyczne mogą żądać od administratora danych sprostowania nieprawidłowości w ich danych osobowych, które są przechowywane. W pewnych okolicznościach, jeśli dane osobowe są niepełne, osoba fizyczna ma prawo wymagać od administratora danych uzupełnienia tych danych lub zarchiwizowania oświadczenia uzupełniającego.

Prawo do przenoszenia danych

Prawo do dostępu do danych przewidziane w RODO daje już osobom fizycznym prawo do otrzymania dotyczących ich danych w powszechnie stosowanym formacie elektronicznym.

Przenoszenie danych wykracza poza ten zakres i wymaga od administratora dostarczenia danych w ustrukturyzowanym, powszechnie stosowanym i nadającym się do odczytu maszynowego formacie, aby osoba, której dane dotyczą mogła przenieść swoje dane osobowe do innego administratora bez przeszkód. Ponadto, administrator danych może zostać zobowiązany do przesłania danych bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. RODO zachęca do stworzenia interoperacyjnych formatów.

O ile prawo dostępu do danych jest uprawnieniem bardzo szerokim, prawo do przenoszenia ma zakres węższy. Dotyczy ono:

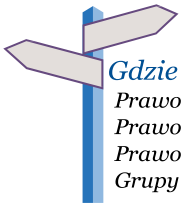
- danych osobowych, które są przetwarzane w sposób zautomatyzowany (bez rejestrów w formie papierowej);
- danych osobowych, które osoba, której dane dotyczą, dostarczyła administratorowi danych; oraz
- wyłącznie sytuacji, w której podstawą prawną przetwarzania jest wyraźna zgoda, lub gdy dane są przetwarzane w celu realizacji umowy lub czynności zmierzających do zawarcia umowy.

Zwrot „dane dostarczone" przez osobę, której dane dotyczą jest interpretowany szeroko. Zgodnie z wytycznymi Grupy Roboczej nie chodzi tu wyłącznie o formularze wypełnione przez osobę fizyczną, ale o wszelkie informacje zebrane przez administratora danych w kontaktach z daną osobą fizyczną lub w wyniku śledzenia jej zachowań. Przykładowo, prawo do przenoszenia danych będzie miało zastosowanie w przypadku: (i) danych zbieranych przez streamingowe serwisy muzyczne, (ii) tytułów książek przetwarzanych przez księgarnię online, (iii) danych zebranych przez inteligentne liczniki lub inne połączone urządzenia, (iv) zapisów (logów) o zachowaniu, (v) historii korzystania ze strony internetowej, (vi) wyszukiwania w internecie, jak również (vii) wiadomości e-mail wysyłanych do osób, których dane dotyczą. Jednakże, prawo do przenoszenia danych nie rozciąga się na dane osobowe wywnioskowane lub wywiedzione przez administratora (przykładowo wyniki algorytmicznej analizy zachowań jednostki).

Podczas gdy prawo do przenoszenia danych będzie miało zastosowanie wyłącznie do administratorów danych, podmioty przetwarzające będą zobowiązane na podstawie postanowień umownych do wspierania administratorów „przez odpowiednie środki techniczne i organizacyjne", aby odpowiadać na żądania przeniesienia danych. Dlatego administratorzy razem z podmiotami przetwarzającymi powinni wdrożyć odpowiednie procedury umożliwiające odpowiadanie na żądania osób, których dane dotyczą.

Prawo do przenoszenia danych nie może powodować uszczerbku dla praw innych osób, których dane dotyczą. Zgodnie jednak z informacjami przekazywanymi przez organy ochrony danych, pierwotny administrator danych nie będzie odpowiadał za przestrzeganie przepisów przez administratora, któremu dane są przekazywane. Zamiast tego, każda organizacja otrzymująca dane musi zapewnić, że wykorzystuje dane zgodnie z prawem. Przewidziano jednak wyjątki od prawa do przenoszenia danych – przykładowo, jeżeli przeniesienie danych mogłoby naruszyć prawa własności intelektualnej lub tajemnicę przedsiębiorstwa. Zdaniem organów ochrony danych nie powinno to jednak uzasadniać zwolnienia z obowiązku realizowania tego prawa

Wymogi związane z przenoszeniem danych mogą również kolidować z wymaganiami dotyczącymi prawa dostępu do oraz przenoszenia danych uregulowanymi w przepisach sektorowych UE (np. prawo dostępu do historii rachunku bankowego przewidziane w drugiej Dyrektywie w sprawie usług płatniczych (UE) 2015/2366 (PSD2)) lub w przepisach państw członkowskich. Zgodnie z wytycznymi Grupy Roboczej prawo do przenoszenia danych nie będzie miało zastosowania, gdy dana osoba oświadczy, że wykonuje przysługujące jej prawa na podstawie innych przepisów. W przypadku jednak, gdy dana osoba chce skorzystać z przysługujących jej praw na podstawie RODO, administrator, w każdym indywidulanym przypadku, powinien dokonać oceny wzajemnego stosunku nachodzących na siebie praw, przy czym przepisy szczególne nie będą automatycznie wykluczały skorzystania przez jednostkę z praw przysługujących jej na podstawie RODO.



Gdzie mogę to znaleźć?

Prawo sprzeciwu art. 15, motywy 59, 63 i 64
Prawo do sprostowania art. 16
Prawo do przenoszenia danych art. 20 i opinia Grupy Roboczej WP 242, motyw 68

Prawo do sprzeciwu

Na pierwszy rzut oka

- Istnieją prawa przysługujące osobom fizycznym w zakresie sprzeciwu wobec określonych rodzajów przetwarzania danych:
  - Przetwarzania dla celów marketingu bezpośredniego;
  - Przetwarzania opartego na prawnie uzasadnionym interesie lub realizacji zadań w interesie publicznym/w ramach sprawowania władzy publicznej; oraz
  - Przetwarzania dla celów badawczych lub statystycznych
- Charakter bezwzględny ma wyłącznie prawo do sprzeciwu wobec przetwarzania danych dla celów marketingu bezpośredniego (tzn. nie trzeba wykazywać podstaw sprzeciwu, nie ma odstępstw, które pozwalałyby na kontynuowanie przetwarzania danych dla tego celu).
- Istnieją obowiązki w zakresie powiadamiania osób fizycznych o przysługujących im prawach na wczesnym etapie - w sposób jasny i oddzielnie od innych rodzajów informacji.
- Usługi internetowe muszą umożliwiać wyrażenie sprzeciwu w sposób zautomatyzowany

Co trzeba zrobić

- Należy dokonać przeglądu informacji dla osób, których dane dotyczą oraz stosownych polityk w celu zapewnienia, że osoby fizyczne są poinformowane o przysługujących im prawach sprzeciwu w sposób jasny i oddzielny od innych informacji, w momencie „pierwszej komunikacji".
- W przypadku usług w Internecie, należy zapewnić, że istnieje zautomatyzowany sposób wykonania powyższego obowiązku; oraz
- Należy dokonać przeglądu wykazów adresów blokowanych oraz procesów (w tym prowadzonych w imieniu Państwa organizacji przez partnerów i usługodawców) w celu zapewnienia, że są oni zdolni do działania w zgodności z przepisami RODO.

Prawo do sprzeciwu

Prawa do sprzeciwu wynikają z przepisów RODO. Wszystkie te prawa odnoszą się do przetwarzana dla określonych celów, lub przetwarzania na określonej podstawie prawnej. Nie przewiduje się prawa osoby fizycznej do sprzeciwu wobec przetwarzania danych w ogóle.

Przewidziane są prawa do sprzeciwu wobec:

Przetwarzania dla celów marketingu bezpośredniego

Jest to prawo o charakterze bezwzględnym; po wyrażeniu sprzeciwu dane nie mogą być dalej przetwarzane dla celów marketingu bezpośredniego.

Przetwarzania dla celów badań naukowych / historycznych lub dla celów statystycznych

Wyżej wspomniane prawo jest mniej restrykcyjne, niż prawo do sprzeciwu wobec marketingu bezpośredniego – muszą istnieć „przyczyny związane z jej [osoby, której dane dotyczą] szczególną sytuacją".

Istnieje odstępstwo dotyczące przypadków, gdy przetwarzanie jest niezbędne dla realizacji zadań na rzecz interesu publicznego.

Przepis ten nie posiada żadnego odpowiednika w dyrektywie w sprawie ochrony danych

Przetwarzania opartego na dwóch określonych podstawach prawnych:

Z tego prawa można korzystać w odniesieniu do sytuacji danej osoby, której dane dotyczą, gdy podstawę prawną przetwarzania stanowi:

1. prawnie uzasadniony interes (tj. na mocy art. 6(1)(f)); lub
2. konieczność dla realizacji zadania w ramach ochrony interesu publicznego lub sprawowania władzy (tj. na mocy art. 6(1)(e))

Administrator jest w takim przypadku zobowiązany zaprzestać przetwarzania danych osobowych chyba, że:

- może powołać się na ważne podstawy, które są nadrzędne w stosunku do interesów osoby, której dane dotyczą; lub
- przetwarzanie służy do ustalenia, dochodzenia lub obrony roszczeń.

Zatem po otrzymaniu od danej osoby sprzeciwu, w odniesieniu do szczególnej, indywidualnej sytuacji tejże osoby, administrator musi samodzielnie ustalić dlaczego powinien pomimo zgłoszonego sprzeciwu nadal mieć możliwość przetwarzania danych osobowych na tej podstawie.

Powyższy przepis stanowi zacieśnienie zasad przewidzianych w dyrektywie w sprawie ochrony danych. W odpowiednim przepisie dyrektywy to osoba, której dane dotyczą, musi wykazać przyczyny swojego sprzeciwu, a przetwarzanie musi zostać wstrzymane jeśli sprzeciw okaże się uzasadniony.

Powiadamianie osób fizycznych o przysługujących im prawach

W przypadku przetwarzania dla celów marketingu bezpośredniego oraz przetwarzania w ramach realizacji zadań na rzecz ochrony interesu publicznego lub prawnie uzasadnionych interesów, osoba fizyczna musi być wyraźnie poinformowana o przysługującym jej prawie do sprzeciwu, najpóźniej w momencie pierwszego kontaktu ze wspomnianą osobą. Musi to być wykonane w sposób jasny i oddzielnie od innych rodzajów informacji

Wyżej wspomniany obowiązek do poinformowania osób nie dotyczy przetwarzania dla celów badawczych lub statystycznych.

W przypadku usług w internecie, osoba fizyczna musi mieć możliwość skorzystania z przysługującego jej prawa w sposób zautomatyzowany.

Gdzie mogę to znaleźć?
art. 21
motywy 69 i 70

Prawo do usuwania i ograniczenia przetwarzania

Na pierwszy rzut oka

- Wprowadzone zostały także bardziej rozległe i niejasne prawa: prawo do bycia zapomnianym (zwane obecnie prawem do usunięcia danych) i prawo do ograniczenia przetwarzania.
- Osoby fizyczne są uprawnione do żądania „usunięcia" danych w przypadku, gdy pojawi się problem z legalnością procesu przetwarzania, lub w przypadku wycofania zgody na przetwarzanie danych.
- Osoba fizyczna ma prawo wymagać od administratora danych „ograniczenia" przetwarzania danych w czasie rozpatrywania skarg (np. w zakresie prawidłowości), lub w przypadku, gdy przetwarzanie jest niezgodne z prawem, ale osoba sprzeciwia się usunięciu danych.
- Administratorzy, którzy dokonali upublicznienia danych, a następnie osoba, której dane dotyczą skorzystała z prawa do żądania usunięcia danych, są zobowiązani do poinformowania innych podmiotów przetwarzających te dane o żądaniu. Będzie to nowy, szeroko zakrojony i kłopotliwy obowiązek.

Co trzeba zrobić

☐	Należy zapewnić, że pracownicy i dostawcy, którzy mogą otrzymywać żądania usunięcia danych, są ich świadomi i wiedzą jak z nimi postępować.
☐	Należy przeanalizować, czy działają Państwo w takim sektorze, gdzie zgodność z wymogami w zakresie usuwania danych byłaby w takim stopniu nieuzasadniona, że należy ubiegać się o dodatkowe ustępstwa ze strony danego państwa członkowskiego.
☐	Należy sprawdzić, czy systemy są w stanie sprostać wymogom oznaczania danych jako zastrzeżone podczas rozpatrywania skarg: w razie potrzeby należy podjąć odpowiednie kroki.

Prawo do bycia zapomnianym

Osobom fizycznym przysługuje prawo do „usunięcia" dotyczących ich danych w pewnych określonych sytuacjach - co do zasady w przypadkach, gdy przetwarzanie nie spełnia wymogów przewidzianych w RODO. Przedmiotowe prawo może być wykonywane wobec administratorów, którzy muszą udzielić odpowiedzi bez zbędnej zwłoki (w każdym przypadku nie później, niż w ciągu jednego miesiąca, jednak termin ten może zostać w niektórych przypadkach wydłużony).

W jakich przypadkach można skorzystać z tego prawa?

- Kiedy dane nie są już potrzebne w związku z celem, dla którego zostały pierwotnie zebrane lub przetwarzane.
- W przypadku, gdy osoba fizyczna wycofa wyrażoną zgodę (oraz jeśli nie ma już uzasadnienia dla przetwarzania).
    - Istnieje jeszcze jedna przesłanka odnosząca się do wycofania zgody wyrażonej uprzednio przez dziecko w związku z usługami w internecie. Jednakże wydaje się, że nie zmienia to generalnej zasady, w myśl której zgoda może zostać wycofana, i w takim przypadku osoba fizyczna ma prawo żądać usunięcia danych.
- W przypadku przetwarzania opartego na prawnie uzasadnionym interesie - jeśli osoba wyrazi sprzeciw a administrator danych nie będzie w stanie wykazać, że istnieją nadrzędne, ważne podstawy dla przetwarzania.
- W przypadku, gdy dane są w inny sposób przetwarzane niezgodnie z prawem (np. w sposób niezgodny z przepisami RODO).
- W przypadku, gdy dane muszą zostać usunięte na podstawie prawa unijnego lub krajowego, które ma zastosowanie do administratora danych.

Ostatni warunek może, mieć zastosowanie w przypadku, gdy osoba fizyczna uzna, że administrator danych osobowych przechowuje dane, pomimo że przepisy prawa wymagają, aby dane te (np. kontrola związana z zatrudnieniem) powinny zostać usunięte po upłynięciu określonego czasu.

Żądania usunięcia danych w sytuacji, gdy dane są przetwarzane „niezgodnie z prawem" są potencjalnie kłopotliwe: istnieje wiele przyczyn, dla których może zostać stwierdzone, że dane są przetwarzane niezgodnie z prawem na mocy RODO (np. dane mogą być nieprawidłowe, jakiś element obowiązkowej informacji nie został uwzględniony w komunikacie przesłanym do danej osoby, itd.). Jednakże nie jest oczywiste, że powinno to zawsze stanowić podstawę do usunięcia danych. Odpowiedni przepis w dyrektywie w sprawie ochrony danych pozostawia więcej pola do manewru wymagając usunięcia danych „w uzasadnionych przypadkach". Należy uważnie obserwować sposób, w jaki państwa członkowskie zaprojektują odstępstwa od tej zasady.

Dane, które stały się częścią domeny publicznej

W przypadku, gdy administrator udostępnił pewne dane osobowe publicznie i jest zobowiązany do usunięcia wspomnianych informacji, administrator danych jest także zobowiązany poinformować pozostałych administratorów, którzy dokonują przetwarzania tych danych o fakcie, że osoba, której dane dotyczą, zażądała usunięcia danych. To zobowiązanie ma na celu wzmocnienie pozycji osoby fizycznej w środowisku cyfrowym.

W odniesieniu do tego obowiązku trzeba będzie podjąć uzasadnione kroki i uwzględnić dostępne technologie oraz koszty ich wdrożenia. Jednakże obowiązek ten jest potencjalnie rozległy i bardzo trudny do zrealizowania: na przykład ze względu na fakt, że dane stały się częścią domeny publicznej, pojawia się pytanie, w jaki sposób pierwotny administrator danych zidentyfikuje innych administratorów, których jest zobowiązany powiadomić.

Pozostałe obowiązki w zakresie powiadamiania odbiorców

W przypadku, gdy administrator jest zobowiązany do usunięcia danych osobowych, administrator jest także zobowiązany powiadomić wszystkie osoby, którym przedmiotowe dane zostały ujawnione, chyba że byłoby to niemożliwe, lub wymagałoby podjęcia nieproporcjonalnych środków.

Odstępstwa

Obowiązek nie ma zastosowania w przypadku, gdy przetwarzanie danych jest konieczne;

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wykonania obowiązku prawnego wynikającego z przepisów unijnych lub krajowych;
- do wykonania zadania w ramach ochrony interesu publicznego lub sprawowania władzy publicznej;
- ze względów zdrowia publicznego;
- dla celów archiwalnych, badawczych lub statystycznych (jeśli spełnione są warunki konieczne dla tego rodzaju przetwarzania); lub
- do ustalenia, dochodzenia lub obrony roszczeń.

W części poświęconej wyjątkom i warunkom szczególnym znajduje się więcej informacji na temat możliwości stosowania odstępstw - jeśli takowe są przewidziane w przepisach prawa UE lub prawa danego państwa członkowskiego.

Prawo do ograniczenia przetwarzania danych

Prawo do ograniczenia przetwarzania danych zastępuje przepisy zawarte w dyrektywie w sprawie ochrony danych dotyczące „blokowania". W pewnych sytuacjach prawo to stwarza alternatywę dla żądania usunięcia danych, a w innych przypadkach umożliwia osobie fizycznej żądanie utrzymywania danych w stanie zawieszenia podczas rozpatrywania innych kwestii.

Czym jest ograniczenie?

Jeśli dane osobowe zostaną ograniczone, administrator będzie mógł je tylko przechowywać. Nie może natomiast dalej przetwarzać danych chyba, że:

- osoba wyrazi na to zgodę; lub
- przetwarzanie jest konieczne w celu ustalenia itd. roszczenia, ochrony praw innej osoby fizycznej lub prawnej, lub ze względu na ważny (unijny lub krajowy) interes publiczny.

W przypadku zautomatyzowanego przetwarzania danych, ograniczenie należy wprowadzić za pomocą środków technicznych a następnie odnotować w systemach IT administratora. Może to oznaczać przeniesienie danych do osobnego systemu, tymczasowe zablokowanie danych na stronie internetowej lub w inny sposób uniemożliwienie dostępu do danych.

W przypadku, gdy dane zostały ujawnione innym osobom, administrator jest zobowiązany powiadomić tych odbiorców o ograniczeniu przetwarzania (chyba, że byłoby to niemożliwe, lub wymagałoby podjęcia nieproporcjonalnych środków).

Administrator jest zobowiązany poinformować osobę fizyczną przed zdjęciem ograniczenia.

Kiedy stosuje się ograniczenie przetwarzania danych?

- W przypadku, gdy osoba fizyczna zakwestionuje poprawność danych, dane osobowe podlegają ograniczeniu przetwarzania przez okres rozpatrywania zgłoszenia;
- W przypadku, gdy osoba fizyczna wyraziła sprzeciw wobec przetwarzania (na podstawie prawnie uzasadnionego interesu), osoba ta może żądać ograniczenia przetwarzania danych przez okres rozpatrywania podstaw przetwarzania;
- W przypadku, gdy przetwarzanie jest niezgodne z prawem, ale osoba fizyczna sprzeciwia się usunięciu danych i żąda ograniczenia przetwarzania; oraz
- W przypadku, gdy administrator nie potrzebuje już danych, ale osoba fizyczna potrzebuje tychże danych do ustalenia, dochodzenia lub obrony roszczeń

Ostatni warunek może, na przykład, oznaczać, że administratorzy będą zobowiązani do przechowywania danych byłych klientów w przypadku, gdy dane osobowe są potrzebne dla celów prowadzonych postępowań, w których osoby te uczestniczą.

Gdzie mogę to znaleźć?

Prawo do usunięcia *art. 17 i 19, motywy 65, 66 oraz 73*
Prawo do ograniczenia przetwarzania *art. 18 i 19, motywy 67 i 73*

Profilowanie i zautomatyzowane podejmowanie decyzji

Na pierwszy rzut oka

- Zasady zautomatyzowanego podejmowania decyzji są podobne do odpowiednich przepisów dyrektywy w sprawie ochrony danych (propozycje wprowadzenia ograniczeń wszystkich rodzajów „profilowania" ostatecznie nie weszły w zakres finalnej wersji RODO).
- Zasady dotyczą decyzji:
  - podejmowanych wyłącznie na podstawie zautomatyzowanego przetwarzania; oraz
  - wywołujących skutki prawne, lub mających podobnie istotny wpływ.
- W przypadku, gdy decyzja:
  - jest konieczna do zawarcia lub wykonania umowy; lub
  - jest dozwolona przepisami prawa UE lub prawa danego państwa członkowskiego mającego zastosowanie do administratora danych; lub
  - opiera się na wyraźnej zgodzie osoby

  można zastosować zautomatyzowane przetwarzanie danych w celu podjęcia decyzji. Jednakże nadal należy zapewnić odpowiednie środki ochrony interesów danej osoby.
- Istnieją dodatkowe ograniczenia profilowania w oparciu o dane wrażliwe - które wymagają wyraźnej zgody lub gdy profilowanie zostało dopuszczone na gruncie prawa UE lub prawa danego państwa członkowskiego ze względu na ważny interes publiczny.

Co trzeba zrobić

- Należy sprawdzić jakie istotne mechanizmy zautomatyzowanego podejmowania decyzji są stosowane. Należy zidentyfikować wszelkie decyzje, które są podejmowane na podstawie
  - zgody;
  - obowiązujących przepisów prawa;
  - oraz takich, które odnoszą się do danych wrażliwych lub do dzieci.
- W przypadku profilowania opartego na zgodzie, należy zapewnić, że zgoda została udzielona w sposób wyraźny.
- W przypadku profilowania opartego na przepisach prawa, należy sprawdzić czy podstawa prawna znajduje się w przepisach unijnych, czy krajowych; należy bacznie obserwować zmiany wprowadzane przez państwa członkowskie w prawie krajowym w celu odzwierciedlenia przepisów RODO.
- W przypadku, gdy profilowanie opiera się na danych wrażliwych:
  - należy sprawdzić, czy mogą Państwo uzyskać wyraźną zgodę;
  - jeśli nie, będą Państwo musieli ubiegać się w państwie członkowskim lub UE o stworzenie podstawy prawnej dla tego rodzaju przetwarzania.
- W przypadku, gdy profilowanie dotyczy dzieci, należy zasięgnąć profesjonalnej porady - jest to obszar ściśle ograniczony.

Znaczenie profilowania

Profilowanie *„polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się”*.

W trakcie procesu legislacyjnego pojawiły się próby wprowadzenia znacznych ograniczeń na każdą działalność w zakresie profilowania. Jednakże, ostatecznie do tego nie doszło - pomimo, iż Motyw 72 wskazuje, że EROD może wydawać wskazówki dotyczące profilowania.

Ograniczenia zautomatyzowanego podejmowania decyzji wywierających istotny wpływ

Ograniczenia wobec decyzji podejmowanych wyłącznie w ramach zautomatyzowanego przetwarzania danych (co może obejmować także profilowanie) mają zastosowanie w przypadku, gdy decyzje te wywołują skutki prawne, lub w podobny sposób istotnie wpływają na osobę, której dane dotyczą. Motyw 71 zawiera przykład podejmowania decyzji kredytowych i cyfrowej rekrutacji w internecie, wyjaśnia także, że elementem możliwym do zakwestionowania jest w tym przypadku brak ludzkiej interwencji.

Osoby fizyczne mają prawo nie podlegać takim decyzjom (można to interpretować albo jako zakaz tego rodzaju przetwarzania lub dopuszczenie przetwarzania z zastrzeżeniem prawa osób fizycznych do sprzeciwu. Ta niejednoznaczność jest także obecna w przepisach dyrektywy w sprawie ochrony danych i państwa członkowskie nie są zgodne co do tej kwestii).

Zautomatyzowane przetwarzanie danych można stosować w przypadku, gdy:

- jest to konieczne w celu zawarcia lub wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą;
- jest to dozwolone przepisami prawa UE lub prawa danego państwa członkowskiego; lub
- jest to oparte na wyraźnej zgodzie osoby.

Profilowanie oparte na wyraźnej zgodzie lub wykonaniu umowy

W pierwszym i trzecim przypadku (wykonanie umowy i zgoda), administrator musi wprowadzić odpowiednie środki zabezpieczające prawa osoby, której dane dotyczą. Powyższe musi obejmować przynajmniej prawo do ludzkiej interwencji mające na celu umożliwienie osobie, której dane dotyczą, wyrażenia swojej opinii i zakwestionowania decyzji.

Odpowiednie przepisy zawarte w dyrektywie w sprawie ochrony danych stwierdzały, że nie jest wymagane, aby skutkiem tej decyzji było spełnienie żądania osoby. Nie zostało to jednak przeniesione do treści RODO, być może ze względu na fakt, że w obszarach takich, jak finanse i ubezpieczenia, o ile tylko zaproponuje się zawarcie umowy (nawet na trudnych warunkach), administrator danych może stwierdzić, że żądanie osoby zostało spełnione, w ten sposób unikając objęcia przedmiotowymi przepisami.

Motyw 71 podkreśla, że należy zastosować odpowiednie techniki statystyczne, zapewnić przejrzystość, zapewnić dostępność środków w celu korygowania niepoprawności i ryzyka błędów; oraz że należy zapewnić bezpieczeństwo i zapobiegać dyskryminacji. Motyw 71 stanowi także, że tego typu działania nie powinny być podejmowane w stosunku do dzieci

Dopuszczalność na gruncie przepisów prawa

W drugim przypadku (dopuszczalność na gruncie przepisów prawa) przepisy muszą same w sobie zawierać odpowiednie środki zabezpieczające interesy osoby. Motyw 71 stwierdza, że profilowanie w celu zapewnienia bezpieczeństwa oraz wiarygodności usług w związku z wykrywaniem oszustw i uchylania się od opodatkowania stanowią takie rodzaje zautomatyzowanych decyzji, które mogą być uzasadnione na gruncie prawa UE lub prawa państwa członkowskiego.

Dane wrażliwe

Zautomatyzowane podejmowanie decyzji w oparciu o dane wrażliwe podlega dodatkowym ograniczeniom. Decyzje oparte na tego rodzaju danych mogą być podejmowane wyłącznie:

- za wyraźną zgodą; lub
- gdy przetwarzanie jest niezbędne z punktu widzenia ważnego interesu publicznego i na podstawie prawa unijnego lub krajowego - które musi uwzględniać środki ochrony interesów osoby, której dane dotyczą.
-

Gdzie mogę to znaleźć?
art. 4 pkt 4 i art. 22
motywy 71 i 72

Obowiązki w zakresie zarządzania danymi

Na pierwszy rzut oka

- RODO wymaga, aby wszystkie organizacje wdrożyły szeroki zakres środków mających na celu zredukowanie ryzyka naruszenia przepisów RODO oraz wykazanie, że poważnie traktują kwestie zarządzania danymi.
- Powyższe obejmuje rozwiązania w ramach rozliczalności, np.: oceny skutków dla ochrony danych, audyty, przeglądy polityki, rejestry działalności oraz (ewentualnie) powołanie inspektora ochrony danych.
- Dla tych organizacji, które dotychczas nie przeznaczały środków budżetowych i osobowych dla celów zgodności z przepisami o ochronie danych, te wymogi będą stanowić duży ciężar.

Stopień zmian

Co trzeba zrobić

- Należy przeznaczyć środki osobowe i budżetowe dla celów zgodności z przepisami o ochronie danych w obrębie Państwa organizacji. Bez względu na to, czy postanowią Państwo powołać inspektora ochrony danych, długa lista środków w ramach zarządzania danymi przewidziana w RODO wymusza posiadanie odpowiednich zasobów na powyższe cele.
- Należy zapewnić, że bez względu na to, czy osoby, na które nałożono odpowiedzialność za bezpieczeństwo danych, niezależnie od tego czy pełnią funkcję inspektora ochrony danych (z punktu widzenia przepisów RODO), czy też nie, posiadają status właściwy inspektorowi ochrony danych, jaki przewidują przepisy RODO.
- Należy rozważyć ścieżki sprawozdawczości - organy nadzoru będą oczekiwać sprawozdawczości bezpośrednio od zarządu. Należy także przyjrzeć się zakresowi obowiązków osób odpowiedzialnych za bezpieczeństwo danych.
- Należy zapewnić, że dla Państwa organizacji został opracowany pełny program zgodności obejmujący elementy takie, jak: oceny skutków dla ochrony danych, regularne audyty, przeglądy polityki kadrowej, aktualizacje, a także szkoleniowe i edukacyjne programy rozwojowe.
- Należy dokonać przeglądu istniejących umów z dostawcami oraz uaktualnić formularze zapytań ofertowych i umowy z dostawcami w celu uwzględnienia obowiązków spoczywających na podmiotach przetwarzających przewidzianych w RODO.
- Należy ponadto monitorować publikacje organów nadzorczych oraz kodeksów postępowania i dobrych praktyk branżowych i unijnych w celu weryfikacji, czy nadają się do wykorzystania w Państwa organizacji. Jeśli są Państwo dostawcą, powinni Państwo przeanalizować wpływ przepisów RODO na Państwa strukturę kosztów i odpowiedzialności tak, aby nie musieć odpowiadać za zgodność działań Państwa klientów z prawem.
- Należy wdrożyć rejestry przetwarzania danych w Państwa organizacji. Jeśli są Państwo dostawcą, należy opracować strategię postępowania z żądaniami ze strony klientów w zakresie uczestnictwa w opracowywaniu wyżej wspomnianych rejestrów.

RODO chroni pewne koncepcje związane z zarządzaniem danymi, które od jakiegoś czasu są wysławiane przez prawodawców i organy nadzorcze. Te pojęcia będą skutkować powstaniem nowych, istotnych zobowiązań operacyjnych oraz kosztów dla wielu organizacji sektora publicznego i prywatnego.

Na administratorów nakłada się ogólny obowiązek przyjęcia środków technicznych i organizacyjnych w celu sprostania wynikającym z RODO obowiązkom (a także w celu wykazania, że zostało to zrobione). Prowadzenie programu regularnych audytów w połączeniu z innymi środkami, o których mowa poniżej (w szczególności oceną skutków dla ochrony danych), wydaje się być dobrze widziane przez organy nadzorcze odpowiedzialne za egzekwowanie zobowiązań przewidzianych przez RODO.

Najważniejsze obowiązki obejmują:

Uwzględnianie ochrony danych w fazie projektowania

Organizacje muszą wdrożyć techniczne i organizacyjne środki aby wykazać, że dokonały oceny i wdrożyły środki ochrony w obrębie swoich działań przetwarzania danych. W szczególności podnoszona jest tu kwestia odpowiedniej polityki kadrowej, a także pseudonimizacji danych (w celu zapewnienia zgodności z obowiązkami w zakresie minimalizacji danych).

Ocena skutków dla ochrony danych

Ocena skutków dla ochrony danych to ocena mająca za zadanie identyfikację i minimalizację ryzyka niezgodności. Koncepcja nie jest nowa – aktualne wskazówki organów nadzorczych zalecają korzystanie z niej, a kancelaria Bird & Bird oferuje już tego typu oceny dla swoich klientów. Jednakże RODO zawiera formalny wymóg prowadzenia takiej oceny.

W szczególności, administratorzy muszą zapewnić, że ocena skutków dla ochrony danych została przeprowadzona dla każdej czynności przetwarzania „o wysokim ryzyku", zanim czynność ta została podjęta - mierzonej w odniesieniu do ryzyka naruszenia praw i wolności osoby fizycznej.

Przetwarzanie o wysokim ryzyku obejmuje: (i) systematyczne i kompleksowe czynności przetwarzania, w tym profilowanie, które są podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób istotnie wpływających na osobę fizyczną, (ii) przetwarzanie na dużą skalę szczególnych kategorii danych osobowych lub danych dotyczących wyroków skazujących i naruszeń prawa lub (iii) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie (monitoring wizyjny).

Projekt wytycznych Grupy Roboczej wskazuje na inne czynniki, które mogą zwiększyć ryzyko, w tym udział osób wymagających szczególnej opieki (np. dzieci, czy pracowników), porównywanie lub łączenie zestawów danych w nieoczekiwany sposób z perspektywy osoby, której dane dotyczą, przekazywanie danych poza Unię Europejską oraz przetwarzanie, które ma na celu uniemożliwić osobie fizycznej wykonywania prawa lub skorzystania z umowy lub usługi.

Jako konieczne minimum, RODO wymaga, aby ocena skutków dla ochrony danych obejmowała:

- Opis planowanych operacji przetwarzania oraz celów przetwarzania;
- Ocenę (i) potrzeby i proporcjonalności przetwarzania danych oraz (ii) związanego z tym ryzyka dla osób, których dane dotyczą (z perspektywy tych osób); oraz
- Listy środków przyjętych, aby (i) zminimalizować ryzyka (w tym ryzyka niezwiązane z ochroną danych osobowych takie jak naruszenie prawa do wolności myśli oraz prawa do przemieszczania się) oraz (ii) zapewnić zgodność z przepisami RODO.

W przypadku powołania inspektora ochrony danych (patrz poniżej), należy zasięgnąć jego rady przy przeprowadzaniu oceny skutków dla ochrony danych.

Brak jest ustalonego formularza dla przeprowadzenia oceny skutków dla ochrony danych, przy czym jak zauważyła Grupa Robocza, wiele szablonów już istnieje. Co ciekawe, projekt wytycznych na ten temat uwzględnia dwa istotne dokumenty Międzynarodowej Organizacji Normalizacyjnej (ISO) - jeden dotyczący zarządzania ryzykiem, a drugi dotyczący oceny skutków dla ochrony danych w kontekście bezpieczeństwa informacji.

Grupa Robocza w swym projekcie wytycznych wskazuje, że ocena skutków dla ochrony danych jest wymagana tylko dla przetwarzania zainicjowanego po wejściu w życie RODO. Jednakże, w przypadku zmiany ryzyka po wejściu w życie RODO, ocena skutków dla ochrony danych powinna zostać przeprowadzona dla przetwarzania zainicjowanego jeszcze przed wejściem w życie RODO.

W przypadku, gdy w toku przeprowadzonej oceny skutków dla ochrony danych zidentyfikowano wysoki poziom ryzyka, którego nie można obecnie zminimalizować, należy skonsultować się z organem nadzorczym. Są to przypadki, gdy znaczące lub nieodwracalne konsekwencje mogą dotknąć osób, których dane dotyczą bądź, gdy jest oczywiste, że takie ryzyko może zaistnieć. Przepisy RODO zawierają szczególne wskazówki proceduralne dla tego procesu.

W ramach prowadzenia oceny skutków dla ochrony danych, w razie potrzeby administratorzy danych osobowych są zobowiązani do zasięgnięcia opinii osób, których dane dotyczą „oraz ich przedstawicieli". W kontekście przetwarzania danych osobowych pracowników, będzie to zapewne interpretowane jako zobowiązanie do przeprowadzenia konsultacji z radą pracowniczą lub związkami zawodowymi.

Inspektor ochrony danych

Administratorzy i podmioty przetwarzające dane mogą powołać inspektora ochrony danych według własnego uznania. Zobowiązane do tego są:

- Organy publiczne (z niewielkimi wyjątkami) ;

- Wszelkie organizacje, których główna działalność polega na:
  - „*regularnym i systematycznym monitorowaniu*" osób, których dane dotyczą „*na dużą skalę*"; lub
  - zakrojonym „*na dużą skalę*" przetwarzaniu danych wrażliwych lub dotyczących wyroków skazujących i naruszeń prawa; oraz
- Podmioty zobowiązane do tego na podstawie prawa lokalnego (państwa takie, jak Niemcy prawdopodobnie znajdą się w tej kategorii).

Wytyczne Grupy Roboczej mają pomóc w interpretacji pojęć „*główna działalność*", „*regularne i systematyczne monitorowanie*" oraz „*na dużą skalę*". Zgodnie z wytycznymi:

- "*Główna działalność*": może oznaczać działalność, która jest nierozerwalnie związana z osiąganiem zamierzonych celów przez administratora danych lub podmiot przetwarzający. W wytycznych potwierdzono, że przetwarzanie danych osobowych pracowników (co z dużym prawdopodobieństwem obejmowałoby dane wrażliwe) jest działalnością uboczną, nie główną. Podane przykłady głównej działalności obejmują monitorowanie przestrzeni publicznej przez firmę ochroniarską, której zlecono takie usługi, szpital przetwarzający dane o stanie zdrowia pacjenta oraz podmiot, któremu zlecono świadczenie usług z zakresu medycyny pracy, przetwarzający dane osobowe pracowników swojego klienta.
- „*Regularne i systematyczne monitorowanie*": Grupa Robocza wymienia tu każdą formę śledzenia online i profilowania, w tym dla celów reklamy behawioralnej i kierowania wiadomości e-mail do określonej grupy odbiorców. Podane przykłady obejmują także: profilowanie i ocenę wiarygodności podmiotu (np. ocena zdolności kredytowej, przeciwdziałanie oszustwom, ocena przysługujących zniżek na ubezpieczenie); śledzenie położenia geograficznego, śledzenie kondycji fizycznej i stanu zdrowia, monitoring wizyjny, przetwarzane danych z wykorzystaniem urządzeń połączonych (inteligentne liczniki, samochody, itp.) oraz czynności marketingowe oparte na danych (t.j. big data).
- "*Na dużą skalę*": W swoich wytycznych Grupa Robocza wskazuje, że nie jest jeszcze gotowa podać konkretnych liczb mających stanowić punkt odniesienia dla tego pojęcia, niemniej jednak opublikowanie konkretnego progu ma nastąpić w najbliższej przyszłości. W wytycznych z grudnia 2016 roku wymieniono kilka dość oczywistych czynników, które należy wziąć pod uwagę dokonując oceny skali działalności danego podmiotu (np. liczba osób objętych przetwarzaniem czy zasięg geograficzny przetwarzania). Podane przykłady przetwarzania na dużą skalę obejmują: bank lub towarzystwo ubezpieczeniowe przetwarzające dane klientów; przetwarzanie przez międzynarodową sieć restauracji fast food danych geolokalizacyjnych klientów w czasie rzeczywistym dla celów statystycznych przez wyspecjalizowany w tym zakresie podmiot przetwarzający.

Wytyczne Grupy Roboczej potwierdzają, że zastosowanie będą miały te same wymogi zarówno w przypadkach, kiedy powołanie inspektora ochrony danych jest dobrowolne, jak i wtedy, gdy powołanie inspektora ochrony danych jest obowiązkowe (podsumowanie wymogów poniżej). Co więcej, jeżeli dana organizacja zdecyduje się na powołanie inspektora ochrony danych, nie może go ograniczać w jego obowiązkach – inspektor ochrony danych musi mieć uprawnienia do dostępu i przeglądania wszystkich przetwarzanych danych. W odpowiedzi na pewne niejasności występujące w RODO, wytyczne Grupy Roboczej potwierdzają, że nic nie stoi na przeszkodzie, aby organizacja powierzyła inspektorowi ochrony danych obowiązek prowadzenia rejestru czynności przetwarzania.

Co istotne, Grupa Robocza rekomenduje również, aby organizacje, które skorzystały z możliwości niepowołania inspektora ochrony danych wykazały, dlaczego uważają, że nie podlegają obowiązkowi powołania inspektora ochrony danych. Taka ocena powinna być aktualizowana i sprawdzana wraz z wprowadzaniem nowych czynności przetwarzania lub usług.

Jeżeli powołanie inspektora ochrony danych nie jest obowiązkowe a dana organizacja nie skorzysta z możliwości dobrowolnego powołania inspektora ochrony danych, pracownik lub zewnętrzny konsultant może zostać wyznaczony do wykonywania podobnych zadań. Grupa Robocza zaleca jednak, aby dla uniknięcia wątpliwości, taka osoba nie była nazywana inspektorem ochrony danych.

W przypadku powołania, inspektor ochrony danych musi posiadać odpowiednie kwalifikacje i wiedzę ekspercką (przy czym na pracodawcy spoczywa obowiązek wsparcia inspektora aby ten utrzymał wiedzę na odpowiednim poziomie). O ile inspektor ochrony danych może być wspierany przez zespół osób, funkcję inspektora ochrony danych może pełnić wyłącznie jedna osoba, najlepiej przebywająca na terenie UE. W wytycznych podkreśla się, że im bardziej wrażliwe dane lub złożone operacje przetwarzania na danych organizacja wykonuje, tym wyższy poziom wiedzy eksperckiej będzie wymagany od inspektora ochrony danych.

Nadrzędnym celem inspektora ochrony danych powinno być zapewnienie zgodności danej organizacji z RODO. Jego zadania powinny obejmować przynajmniej: doradzanie pozostałym pracownikom i czuwanie nad zapewnieniem zgodności organizacji z RODO, z przepisami z zakresu ochrony danych osobowych czy z wewnętrzną polityką m.in. poprzez szkolenia, podnoszenie świadomości, audyty, doradztwo w zakresie oceny skutków dla ochrony danych oraz współpracę z organami nadzorczymi. Wytyczne wskazują, że inspektor ochrony danych nie będzie ponosił odpowiedzialności osobistej za to, że dana organizacja nie spełnia wymogów przewidzianych w RODO. Odpowiedzialność poniesie organizacja, w tym odpowiedzialność za brak wsparcia inspektora ochrony danych w osiągnięciu jego nadrzędnego celu.

Należy zapewnić odpowiednie środki w celu umożliwienia inspektorowi danych osobowych wywiązania się z jego obowiązków wynikających z RODO. Ponadto, inspektor danych osobowych powinien podlegać bezpośrednio kierownictwu najwyższego szczebla.

Spółki należące do jednej grupy kapitałowej mogą wyznaczyć jednego inspektora ochrony danych. Inspektor może być pracownikiem lub zewnętrznym zleceniobiorcą. Wytyczne Grupy Roboczej wskazują, że inspektor ochrony danych powinien posiadać pogłębioną wiedzę o organizacji, którą reprezentuje oraz być dostępny - aby organy nadzorcze jak również osoby, których dane dotyczą (np. klienci i pracownicy) w krajach, w których dana organizacja prowadzi działalność mogły się z nimi łatwo kontaktować,. Wydaje się zatem, że Grupa Robocza oczekuje od inspektorów ochrony danych, że będą nie tylko multi-lingwistami, ale specjalistami od ochrony danych – lub przynajmniej, że będą mieć ułatwiony dostęp do dobrych narzędzi służących do tłumaczeń.

Administratorzy danych oraz podmioty przetwarzające muszą zapewnić, aby inspektor ochrony danych był zaangażowany we wszystkie istotne kwestie dotyczące ochrony danych (w tym, zgodnie z wytycznymi Grupy Roboczej, naruszenie ochrony danych), aby mógł wykonywać swe obowiązki niezależnie, a także aby nie był zwolniony bądź karany za wykonywanie swoich obowiązków. W przyszłości okaże się jak te postanowienia będą interpretowane na gruncie prawa pracy. Organizacje powinny zapewnić bezpieczne i poufne kanały komunikacji pomiędzy pracownikami a inspektorem ochrony danych.

Ponadto, zgodnie z wytycznymi, jeżeli kierownictwo nie zgodzi się z zaleceniami inspektora ochrony danych lub nie zastosuje się do nich, kierownictwo powinno to odnotować i podać przyczyny takiej decyzji. W wytycznych zawarto także ostrzeżenie, że nie wolno wydawać inspektorowi poleceń co do sposobu rozwiązania danej kwestii, rezultatów, które powinny zostać osiągnięte oraz tego czy należy skonsultować się z organem nadzorczym, co może prowadzić do potencjalnych zmian będących następstwem naruszenia ochrony danych osobowych.

RODO nie ogranicza inspektora ochrony danych w zajmowaniu innych stanowisk, ale wymaga aby organizacje zapewniły, że sprawowanie takich innych funkcji nie stanowiło źródła konfliktu interesów dla inspektora ochrony danych. Wytyczne Grupy Roboczej idą nawet dalej w tym zakresie. Wskazano w nich bowiem, że inspektor ochrony danych nie może zajmować stanowisk kierowniczych (takich jak dyrektor generalny, dyrektor ds. operacyjnych czy dyrektor finansowy). Również niższe stanowiska kierownicze, w tym dyrektor działu HR, marketingu czy IT lub nawet stanowiska niższego szczebla, które umożliwiają określanie celów i środków przetwarzania nie powinny być zajmowane przez inspektora ochrony danych. Jeżeli zewnętrzny doradca (np. prawnik) świadczy usługi inspektora ochrony danych na rzecz administratora lub podmiotu przetwarzającego, taka osoba powinna powstrzymać się od reprezentowania tych podmiotów przed sądami w sprawach dotyczących ochrony danych.

Dane kontaktowe inspektora ochrony danych muszą zostać podane do wiadomości oraz zakomunikowane organowi nadzorczemu, któremu organizacja podlega, ponieważ inspektor danych osobowych jest osobą kontaktową dla potrzeb pytań związanych z kwestiami ochrony danych.

Korzystanie z usług zewnętrznych dostawców (podmioty przetwarzające dane)

RODO nakłada na administratorów obowiązek dołożenia najwyższych starań przy wyborze usługodawców na potrzeby przetwarzania danych osobowych, co obejmuje między innymi wymóg regularnego przeglądu procedury przetargowej i zapytań ofertowych.

Umowy muszą być zawierane z takimi usługodawcami, którzy w swojej ofercie uwzględniają szeroki zakres informacji (np. zakres przetwarzanych danych oraz okres ich przetwarzania), a także zakres realizowanych obowiązków (np. pomoc w przypadku naruszenia ochrony danych, zapewnienie odpowiednich środków technicznych i organizacyjnych, jak również obowiązki w zakresie wsparcia podczas audytów). To samo tyczy się przypadków, gdy usługodawca zatrudnia podwykonawcę w celu przetwarzania danych.

Zarówno Komisja Europejska, jak i organy nadzorcze, będą prawdopodobnie publikować zatwierdzone klauzule umowne dla celów zawierania umów z usługodawcami. Wydaje się prawdopodobne, że z punktu widzenia usługodawcy będzie to oznaczało dodatkowe obowiązki. Z tego względu usługodawcy powinni dokonać rewizji swojego podejścia do stawek za swoje usługi.

Rejestrowanie czynności przetwarzania

Organizacje są zobowiązane prowadzić rejestry prowadzonych przez siebie czynności przetwarzania informacji (kategorii danych, cel, dla którego są wykorzystywane itd.) podobnie do tego, co na mocy obecnie obowiązujących przepisów administratorzy są zobowiązani zgłaszać organom nadzorczym.

Ponadto, podmioty przetwarzające dane są zobowiązane do prowadzenia rejestrów danych osobowych, które przetwarzają na zlecenie administratorów, co będzie kłopotliwe dla wielu dostawców usług telekomunikacyjnych i usług przetwarzania danych w chmurze.

O ile zwolnienie od powyższego przysługuje organizacjom zatrudniającym mniej, niż 250 osób, nie będzie z niego można skorzystać w przypadku przetwarzania danych wrażliwych, co zniweczy użyteczność tego zwolnienia.

Gdzie mogę to znaleźć?

Uwzględnianie kwestii prywatności na etapie projektowania
art. 25, motywy 74-78

Ocena skutków dla ochrony danych
art. 35-36, motywy 89-94

Inspektorzy ochrony danych
art. 37-39, motywy 97, opinia Grupy Roboczej WP 243

Korzystanie z usług podmiotów przetwarzających dane
art. 28 i 29, motyw 81

Rejestrowanie czynności przetwarzania
art. 30, motyw 82

Naruszenia ochrony danych osobowych i ich zgłaszanie

Na pierwszy rzut oka

- Administratorzy i podmioty przetwarzające dane podlegają teraz przepisom ogólnym w sprawie zgłaszania naruszeń ochrony danych.
- Podmioty przetwarzające dane są zobowiązane zgłaszać naruszenia ochrony danych do administratorów danych.
- Administratorzy danych z kolei są zobowiązani zgłaszać naruszenia ochrony danych do organów nadzorczych, którym podlegają, a w pewnych przypadkach zawiadamiać także do osoby, których dane dotyczą, w każdym przypadku postępując zgodnie z przepisami RODO.
- Administratorzy danych osobowych są zobowiązani prowadzić wewnętrzny rejestr naruszeń ochrony danych.
- Brak zgodności może doprowadzić do nałożenia administracyjnej kary pieniężnej w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która kwota jest wyższa.
- Na obecną chwilę nadal obowiązują przepisy ogólne w zakresie zgłaszania naruszeń ochrony danych dla dostawców usług telekomunikacyjnych, przewidziane w Rozporządzeniu Komisji nr 611/2013 w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektroniczne („Rozporządzenie 611/2013”).

Co trzeba zrobić

- Zgodnie z zasadą rozliczalności wprowadzoną przez RODO, administratorzy danych oraz podmioty przetwarzające dane powinny opracować lub uaktualnić swoje procedury zgłaszania naruszeń ochrony danych, w tym w zakresie systemów identyfikacji incydentów i planów działania.
- Procedury te powinny być regularnie testowane i poddawane przeglądom.
- Powinni Państwo, przy współpracy z jednostkami ds. systemów informatycznych i bezpieczeństwa wewnętrznego swojej organizacji, zapewnić, że wdrożone zostaną odpowiednie techniczne i organizacyjne zabezpieczenia, które spowodują, że w przypadku dostępu osób nieupoważnionych dane staną się niemożliwe do odczytania.
- Ponadto należy dokonać przeglądu polis ubezpieczeniowych aby ocenić zakres ochrony, jaką zapewniają w przypadku naruszenia ochrony danych.
- Wzory umów ramowych / klauzul ochrony danych oraz dokumentacji przetargowej powinny zostać uaktualnione przez klientów, w tym: (i) w celu zobowiązania dostawców do aktywnego zgłaszania naruszeń ochrony danych oraz (ii) położenia większego nacisku na obowiązek współpracy pomiędzy stronami.

Incydenty, które prowadzą do zgłoszenia naruszenia

W przypadku zajścia incydentu określanego, jako „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych", nowe przepisy ogólne w sprawie zgłaszania naruszenia ochrony danych, wprowadzone na mocy RODO, będą obowiązywać w następujący sposób:

1. *Obowiązek podmiotów przetwarzających dane do powiadomienia administratora danych*

Termin:

Bez zbędnej zwłoki po powzięciu wiedzy o zdarzeniu.

Odstępstwo:

Brak na gruncie RODO (jednak EROD ma wydać wytyczne dotyczące *„szczególnych okoliczności, w których administrator lub podmiot przetwarzający jest zobowiązany zgłosić naruszenie ochrony danych osobowych*")

Wnioski:

- Wszystkie naruszenia będzie trzeba zgłaszać.
- EROD ma wydać wytyczne w celu wyjaśnienia pojęcia „zbędnej zwłoki" oraz określonych okoliczności, w których podmiot przetwarzający dane jest zobowiązany zgłaszać naruszenie ochrony danych osobowych.

2. *Obowiązek administratorów danych osobowych do powiadomienia organów nadzorczych*

Termin:

Bez zbędnej zwłoki oraz, w miarę możliwości, nie później, niż 72 godziny po zasięgnięciu wiedzy o zdarzeniu.

Odstępstwo:

Brak obowiązku zgłaszania w przypadku, gdy naruszenie nie jest związane z ryzykiem naruszenia praw i wolności osób fizycznych.

Wnioski:

- W przypadku uchybienia terminom zgłoszenia, będzie konieczne wyjaśnienie sytuacji organom nadzorczym (np. żądanie ze strony organu wymiaru sprawiedliwości)
- EROD ma wydać wytyczne w celu wyjaśnienia pojęcia „zbędnej zwłoki" oraz określonych okoliczności, w których administrator danych jest zobowiązany zgłaszać naruszenie ochrony danych osobowych

3. *Obowiązek administratorów danych osobowych powiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych*

W przypadku, gdy działanie takie nie zostało podjęte, organ nadzorczy może zobowiązać administratora danych osobowych do powiadomienia o naruszeniu ochrony danych osobowych osób, których dane dotyczą, chyba że zastosowanie ma jedno z trzech odstępstw.

Termin:

Bez zbędnej zwłoki: konieczność zminimalizowania natychmiastowego ryzyka szkód wymaga szybkiego kontaktu z osobami, których dane dotyczą, natomiast konieczność wdrożenia odpowiednich środków przeciwko trwającym lub podobnym naruszeniom ochrony danych może uzasadniać dłuższy okres na zgłoszenie.

Odstępstwo:

Brak konieczności zgłaszania w przypadku:

- Gdy naruszenie nie jest związane z ryzykiem naruszenia praw i wolności osób, których dane dotyczą, albo takie ryzyko jest niższe niż wysokie;
- Gdy odpowiednie techniczne i organizacyjne zabezpieczenia były wdrożone w chwili zajścia incydentu (np. szyfrowanie danych); lub
- Gdyby spowodowało to konieczność podjęcia nieproporcjonalnie dużych starań (zamiast tego powinno się organizować publiczne kampanie informacyjne w celu skutecznego informowania dotkniętych problemem osób)

Wymagania w zakresie dokumentacji

- Wewnętrzny rejestr naruszeń: administrator jest zobowiązany dokumentować wszelkie naruszenia ochrony danych osobowych *„w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze*". Możliwe jest zawnioskowanie do organu nadzorczego o dokonanie oceny sposobu, w jaki administratorzy danych wywiązują się ze swoich obowiązków w zakresie zgłaszania naruszenia ochrony danych.
- Istnieją także ustalone wymogi w zakresie powiadamiania organów nadzorczych (np. dotyczące opisywania charakteru naruszenia ochrony danych osobowych, w tym, w razie możliwości, kategorii i przybliżonej liczby osób, których dane dotyczą objętych zakresem naruszenia, a także kategorii i przybliżonej liczby rejestrów danych objętych zakresem naruszenia, itd.) jak również powiadamiania osób objętych zakresem naruszenia (np. w zakresie opisania jasnym i prostym językiem charakteru naruszenia ochrony danych osobowych oraz zapewnienia informacji w zakresie nie mniejszym, niż: (i) imienia, nazwiska i danych kontaktowych inspektora ochrony danych lub innej osoby kontaktowej która może udzielić dalszych informacji; (ii) możliwych konsekwencji naruszenia ochrony danych osobowych; oraz (iii) środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków).

Sankcje w przypadku nieprzestrzegania przepisów

Za niesprostanie wyżej wymienionym wymogom grozi administracyjna kara pieniężna w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa, do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która kwota jest wyższa.

A co z innymi przepisami ogólnymi Unii w zakresie zgłaszania naruszenia ochrony danych osobowych przez dostawców usług telekomunikacyjnych?

W chwili obecnej Rozporządzenie nr 611/2013 - które przewiduje określoną procedurę zgłaszania naruszeń (opisaną w Dyrektywie 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej („dyrektywa o prywatności i łączności elektronicznej")) – nadal obowiązuje dostawców publicznie dostępnych usług telekomunikacyjnych (np. przedsiębiorców telekomunikacyjnych, dostawców usług internetowych i usług w zakresie poczty elektronicznej). Jednakże, 10 stycznia 2017 r. Komisja Europejska opublikowała projekt rozporządzenia w sprawie prywatności i łączności elektronicznej.

Okoliczność, że powyższe rozporządzenie ma wejść w życie w tej samej dacie co RODO symbolizuje zamierzone powiązanie pomiędzy tymi aktami. Rozporządzenie w sprawie prywatności i łączności elektronicznej uchyla wprawdzie dyrektywę o prywatności i łączności elektronicznej, ale zawiera jednocześnie regulacje o podobnym brzmieniu dotyczące zgłaszania naruszeń, co wspomniana dyrektywa. Rozporządzenie w sprawie prywatności w łączności elektronicznej nie uchyla jednak Rozporządzenia 611/2013. W praktyce zatem, dostawcy usług telekomunikacyjnych będą zobligowani do zgłaszania naruszeń właściwym organom nadzorczym także na podstawie przepisów Rozporządzenia 611/2013. Naszym jednak zdaniem, Rozporządzenie 611/2013 zostanie uchylone na korzyść przepisów RODO.

Gdzie mogę to znaleźć?
motywy 85-88, art. 33, 34, 70, 83 i 84

Kodeksy postępowania i certyfikacja

Na pierwszy rzut oka

RODO uwzględnia w swoich przepisach zatwierdzanie kodeksów postępowania („Kodeksy") oraz możliwość akredytowania podmiotów certyfikujących, a także znaków jakości i oznaczeń aby pomóc administratorom w wykazaniu zgodności i stosowania najlepszych praktyk.

Kodeksy postępowania:

- Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać Kodeksy do zatwierdzenia, rejestracji i publikacji przez organy nadzorcze lub, w przypadku przetwarzania danych w różnych państwach członkowskich, przez Europejską Radę Ochrony Danych. Komisja Europejska może ponadto orzec, że Kodeksy rekomendowane przez EROD obowiązują na całym terytorium UE.
- Kodeksy mogą być zatwierdzane w odniesieniu do szerokiego zakresu zagadnień, a ich przestrzeganie pomoże administratorom i podmiotom przetwarzającym dane w wykazaniu zgodności z przepisami RODO.
- Zgodność z Kodeksami będzie monitorowana, a działania w tym zakresie mogą być realizowane przez odpowiednio wykwalifikowane i akredytowane podmioty. Administratorzy i podmioty przetwarzające dane, którzy naruszają przepisy Kodeksów mogą zostać ukarani wykluczeniem z grona sygnatariuszy Kodeksu oraz zgłoszeniem naruszenia do organu nadzorczego.

Mechanizmy certyfikacji, znaki jakości i oznaczenia:

- Zachęca się do ustanawiania, w odniesieniu do ochrony danych osobowych, mechanizmów certyfikacji, znaków jakości i oznaczeń.
- Certyfikaty będą wystawiane przez akredytowane podmioty certyfikujące (które dopiero powstaną).
- Certyfikacja jest dobrowolna, jednak pozwoli ona administratorom danych i podmiotom przetwarzającym dane na wykazanie zgodności z przepisami RODO.
- Certyfikaty będą ważne przez trzy lata z możliwością przedłużenia.
- EROD będzie prowadzić ogólnodostępny rejestr wszystkich mechanizmów certyfikacji, znaków jakości i oznaczeń.

Co trzeba zrobić

Kodeksy postępowania

- Aby zapewnić sobie przewagę jeszcze przed ustanowieniem procedury akredytacji przez organy nadzorcze, podmioty przetwarzające dane (np. dostawcy usług w zakresie przechowywania danych w chmurze) i administratorzy danych w określonych sektorach powinni rozważyć zidentyfikowanie lub zawiązanie stowarzyszeń lub organów przedstawicielskich, które mogłyby opracować Kodeksy do zatwierdzenia przez organy nadzorcze.

Mechanizmy certyfikacji, znaki jakości i oznaczenia

- Podmioty przetwarzające dane i administratorzy danych osobowych powinni śledzić rozwój sytuacji w kontekście akredytowania podmiotów certyfikujących i rozważyć, czy w odpowiednim czasie będą ubiegać się o certyfikację.
- Po ustanowieniu programów certyfikacji, administratorzy powinni zapoznać się z założeniami tych programów i uwzględnić kwestię certyfikacji, a także znaki jakości i oznaczenia dokonując wyboru podmiotów przetwarzających dane lub usługodawców.

Kodeksy postępowania

Kodeksy są istotnym elementem poszerzania i dostosowywania narzędzi służących do zapewniania zgodności z przepisami o ochronie danych, które administratorzy i podmioty przetwarzające dane mogą wykorzystywać w charakterze mechanizmu samo-samoregulacji.

Oczekuje się, że Kodeksy będą dostarczać miarodajnych wytycznych w zakresie pewnych istotnych obszarów, w tym:

- prawnie uzasadnionych interesów w określonych kontekstach;
- pseudonimizacji;
- korzystania przez osoby, których dane dotyczą, z przysługujących im praw;
- ochrony nieletnich i wyrażania zgody rodzicielskiej;
- uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, a także środków bezpieczeństwa danych;
- zgłaszania naruszenia ochrony danych; oraz
- rozwiązywania sporów pomiędzy administratorami danych a osobami, których dane dotyczą.

Opracowywanie i zatwierdzanie Kodeksów prawdopodobnie przyniesie pewne istotne korzyści, na przykład:

- ustanowienie i uaktualnienie najlepszych praktyk w zakresie zgodności w określonych kontekstach przetwarzania danych;
- umożliwienie administratorom danych i podmiotom przetwarzającym dane zobowiązania się do zachowania zgodności z uznawanymi normami i praktykami, oraz bycia rozpoznawanym jako podmiot, który wspomnianych norm i praktyk przestrzega;
- przestrzeganie Kodeksów może świadczyć o tym, że podmioty odbierające dane (zarówno administratorzy, jak i podmiot y przetwarzające dane), zlokalizowane poza terytorium UE/EOG, wprowadziły odpowiednie zabezpieczenia w celu umożliwienia przekazywania danych na mocy art. 46. Przekazywanie danych na podstawie Kodeksu wraz z wiążącymi i egzekwowalnymi zobowiązaniami podmiotu odbierającego dane w zakresie stosowania odpowiednich zabezpieczeń, może się odbywać bez żadnych szczególnych form autoryzacji ze strony organów nadzorczych, a Kodeksy mogą w ten sposób stanowić alternatywę dla innych mechanizmów międzynarodowego przekazywania danych na takim samym poziomie, jak standardowe klauzule umowne i wiążące reguły korporacyjne.

Zatwierdzanie Kodeksów

Kodeksy opracowane przez zrzeszenia lub inne organizacje sektorowe w odniesieniu do operacji przetwarzania danych, które dotyczą jedynie jednego państwa członkowskiego, należy zgłaszać do właściwego organu nadzorczego w celu uzgodnienia oraz, z zastrzeżeniem ewentualnych zmian lub rozszerzeń - zatwierdzenia. W przypadku, gdy Kodeks obejmuje operacje przetwarzania danych w kilku państwach członkowskich, powinien on zostać przedłożony EROD celem zaopiniowania. Z zastrzeżeniem możliwości modyfikacji lub rozszerzenia, zarówno Kodeks, jak i opinia wydana przez EROD, mogą następnie przedłożone Komisji Europejskiej, która, po przeprowadzeniu oceny, może przyznać mu status powszechnie obowiązującego.

Kodeksy powinny być ogólnodostępne w rejestrach publicznych.

Monitorowanie zgodności

Zgodność z Kodeksami będzie monitorowana wyłącznie przez organy akredytowane przez właściwe organy nadzorcze.

W celu uzyskania akredytacji, organy te będą musiały wykazać:

- swoją niezależność, wiedzę i doświadczenie;
- opracowanie procedur mających za zadanie ocenę zdolności administratorów i podmiotów przetwarzających dane do stosowania postanowień Kodeksu, a także do monitorowania zgodności oraz regularnego przeglądu Kodeksu;
- zdolność do rozpatrywania skarg dotyczących naruszeń; a także
- wdrożenie procesów mających na celu zapobieżenie konfliktom interesów.

Akredytacja może zostać cofnięta w przypadku, gdy dany podmiot przestanie spełniać określone warunki.

Mechanizmy certyfikacji, znaki jakości i oznaczenia

Pojęcie certyfikowania operacji przetwarzania danych stanowi ważny krok naprzód w procesie tworzenia wiarygodnych i sprawdzalnych ram dla operacji przetwarzania danych. Jest prawdopodobne, że proces ten będzie szczególnie istotny w kontekście usług w zakresie chmury obliczeniowej i innych form usług wielodostępnych, w przypadku których indywidualne audyty często okazują się rozwiązaniem niepraktycznym.

Państwa członkowskie, organy nadzorcze, EROD oraz Komisja są zachęcane do ustanawiania mechanizmów certyfikacji, znaków jakości i oznaczeń w zakresie ochrony danych w odniesieniu do określonych operacji przetwarzania.

Certyfikacja jest dobrowolna. Właściwe organy nadzorcze lub EROD będą odpowiedzialne za zatwierdzanie kryteriów dla certyfikacji. EROD może opracowywać kryteria dla wspólnego mechanizmu certyfikacji zwanego europejskim znakiem jakości ochrony danych (*European Data Protection Seal*).

Certyfikacja niesie ze sobą dwie główne zalety:

1. administratorzy i podmioty przetwarzające dane będą mogły wykazać zgodność z prawem, w szczególności w odniesieniu do wdrożenia środków technicznych i organizacyjnych.
2. certyfikaty mogą wykazać, że podmioty odbierające dane (administratorzy oraz podmioty przetwarzające dane) zlokalizowane poza terytorium UE/EOG wprowadziły odpowiednie zabezpieczenia dla celów zgodności z przepisami art. 46 oraz że przekazywanie na podstawie mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami podmiotu odbierającego dane do stosowania odpowiednich zabezpieczeń może się odbywać bez szczególnej autoryzacji ze strony organów nadzorczych, a Kodeksy mogą w ten sposób stanowić alternatywę dla innych mechanizmów międzynarodowego przekazywania danych na takim samym poziomie, jak standardowe klauzule umowne i wiążące reguły korporacyjne.

Certyfikaty dla operacji przetwarzania będą wydawane na okres trzech lat z możliwością przedłużenia lub wycofania w przypadku, gdy dany podmiot przestane spełniać właściwe warunki.

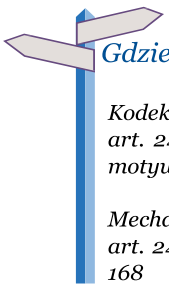
EROD będzie prowadzić ogólnodostępny rejestr obejmujący wszystkie mechanizmy certyfikacji, znaki jakości i oznaczenia.

Certyfikaty mogą być wydawane przez publiczne i prywatne akredytowane podmioty certyfikujące. Krajowe Podmioty Certyfikujące lub organy nadzorcze mogą udzielać akredytacji podmiotom certyfikującym (w celu umożliwienia im wystawiania certyfikatów, znaków jakości i oznaczeń), które (między innymi):

- posiadają wymaganą wiedzę i doświadczenie i są niezależne w odniesieniu do przedmiotu certyfikacji;
- wprowadziły procedury pozwalające na przegląd i wycofanie certyfikacji, znaków jakości i oznaczeń;
- są zdolne rozpatrywać skargi dotyczące naruszeń warunków certyfikacji; oraz
- wprowadziły zasady rozwiązywania konfliktów interesów.

Kryteria dla akredytacji zostaną opracowane przez organy nadzorcze i EROD, a następnie zostaną udostępnione publicznie.

Akredytacje dla podmiotów certyfikujących będą wydawane na okres maksymalnie pięciu lat z możliwością przedłużenia lub wycofania w przypadku, gdy dany podmiot przestane spełniać określone warunki.



Gdzie mogę to znaleźć?

Kodeksy postępowania
art. 24, 28 ust. 5, art. 32, 40, 41, 57, 58, 64, 70, 83, motywy 77, 81, 98, 99, 148, 168

Mechanizmy certyfikacji, znaki jakości i oznaczenia
art. 24, 25, 28, 32, 42, 43, motywy 77, 81, 100, 166 i 168

Przekazywanie danych osobowych do państw trzecich

Na pierwszy rzut oka

- Przekazywanie danych osobowych odbiorcom zlokalizowanym w tzw. „państwach trzecich” (tj. poza terytorium Europejskiego Obszaru Gospodarczego („EOG”) nadal będzie regulowane i w pewnych okolicznościach ograniczane.
- Zobowiązana wynikające z RODO są generalnie podobne do obowiązków przewidzianych w dyrektywie w sprawie ochrony danych, przy czym wprowadzono pewne usprawnienia mechanizmów zapewnienia zgodności, szczególnie w postaci usunięcia konieczności zgłaszania standardowych klauzul umownych do organów nadzorczych, a także zachęty do opracowywania zatwierdzonych kodeksów postępowania w zakresie przekazywania danych i mechanizmów certyfikacji.
- Przestrzeganie przepisów w zakresie ochrony danych nadal będzie istotną kwestią dla organizacji międzynarodowych a także dla wszystkich, którzy korzystają z łańcuchów dostaw, w ramach których przetwarzane są dane osobowe poza terytorium EOG.
- Naruszenie przepisów o przekazywaniu danych przewidzianych w RODO stanowi jedno z naruszeń zagrożonych karą pieniężną w maksymalnej wysokości (do 4% całkowitego, rocznego obrotu).
- Postępowanie w przedmiocie nieprzestrzegania przepisów może zostać wszczęte przeciwko administratorom, jak również podmiotom przetwarzającym dane.

Co trzeba zrobić

- ☐ Należy przejrzeć najważniejsze trasy międzynarodowego przepływu danych i opracować ich mapę.
- ☐ Należy rozważyć, które mechanizmy przekazywania danych są u Państwa wdrożone i czy będą one nadal wystarczające.
- ☐ Należy także poddać rewizji pytania zawarte w standardowych formularzach przetargowych i klauzulach umownych w celu zapewnienia, że informacje na temat przekazywania danych osobowych proponowanego przez Państwa dostawcę, za które ponoszą Państwo odpowiedzialność, są przekazywane zgodnie z obowiązującymi przepisami.
- ☐ W przypadku, gdy w przeszłości Państwo, albo Państwa dostawca, powoływali się na certyfikat *Safe Harbor* w celu zapewnienia odpowiednich środków, należy pamiętać, że rozwiązanie to już nie obowiązuje. Aby uzasadniać ciągłe przekazywanie danych w kontekście transatlantyckim będą Państwo musieli poddać rewizji swoje relacje z dostawcami i klientami w celu wypracowania nowych podstaw prawnych do takiego przekazywania.
- ☐ W odniesieniu do przekazywania danych w obrębie grupy przedsiębiorstw, należy rozważyć czy wiążące reguły korporacyjne będą dobrym rozwiązaniem.
- ☐ W przypadku przetwarzania danych osobowych poza terytorium EOG, przy jednoczesnym dostarczaniu towarów i usług, należy się spodziewać ze strony Państwa klientów pytań o stosunek do zgodności z przepisami zarówno Państwa, jak i Państwa dostawcy.
- ☐ Należy uważnie śledzić rozwój sytuacji w zakresie zatwierdzonych kodeksów postępowania i programów certyfikacji w kontekście działalności Państwa organizacji.

Komentarz

Przekazywanie danych osobowych do „państw trzecich" (tj. poza terytorium EOG) nadal będzie podlegało ograniczeniom wynikającym z RODO. Będzie to nadal istotna kwestia dla wszystkich organizacji międzynarodowych. Jednakże obecnie obowiązujące wymogi w dużej mierze nadal będą obowiązywać, przy czym wprowadzono pewne usprawnienia.

Podstawowym usprawnieniem jest fakt, że aktualnie obowiązujący proces, w ramach którego (w niektórych państwach) przekazywanie danych w oparciu o standardowe klauzule umowne musi być zgłaszane lub zatwierdzane przez organy nadzorcze, został usunięty.

W świetle nowych zasad Komisja będzie uprawniona do stwierdzania, że niektóre państwa, obszary, sektory lub międzynarodowe organizacje zapewniają odpowiedni poziom ochrony w odniesieniu do przekazywania danych. Istniejący wykaz państw, które uzyskały wcześniej aprobatę Komisji, pozostanie w mocy, tzn.: Andora, Argentyna, Kanada (gdzie obowiązuje PIPEDA), Szwajcaria, Wyspy Owcze, Guernsey, Izrael, Wyspa Man, Baliwat Jersey, Wschodnia Republika Urugwaju i Nowa Zelandia. Dodanie lub usunięcie państwa z powyższego wykazu będzie komunikowane w Dzienniku Urzędowym.

Amerykański program *Safe Harbor*, który został w przeszłości zatwierdzony decyzją Komisji, już nie obowiązuje. Jednakże 12 lipca 2016 r., już po 9 miesiącach od unieważnienia programu *Safe Harbor*, Komisja Europejska przyjęła decyzję zatwierdzającą odpowiedni poziom ochrony jego następcy, *EU-US Privacy Shield*. Amerykańskie organizacje mogą same zaświadczać przestrzeganie standardów zawartych w *Privacy Shield* od 1 sierpnia 2016 r. *Privacy Shield* zapewnia Komisji Europejskiej możliwość przeprowadzenia okresowych weryfikacji w celu sprawdzenia poziomu ochrony zapewnianego przez *Privacy Shield*, również po wejściu w życie RODO. W RODO brak jest odniesień wprost do *Privacy Shield*, jednakże RODO obejmuje swoim zakresem najważniejsze wymogi dotyczące oceny stopnia ochrony opisane w decyzji w sprawie *Schrems*.

RODO zawiera znaczną ilość informacji w zakresie konkretnych procedur i kryteriów, które muszą zostać uwzględnione przez Komisję podczas oceny stopnia ochrony, z naciskiem na potrzebę zapewnienia, że tzw. państwa trzecie oferują poziom ochrony, który można opisać jako „*zasadniczo odpowiadający stopniowi ochrony zapewnianemu w Unii*", a także zapewniają osobom, których dane dotyczą, skuteczne i wykonalne prawa i środki naprawcze. Komisja będzie konsultować się z EROD podczas przypisywania poziomów ochrony i zapewni bieżący monitoring i przegląd decyzji podejmowanych w tym kierunku (nie rzadziej, niż raz na cztery lata). Komisja jest ponadto uprawniona do wycofania, zmiany i zawieszenia decyzji podjętych w zakresie poziomu ochrony.

Inne dostępne metody przenoszenia danych osobowych nadal są uznawane: standardowe klauzule umowne (przyjęte przez Komisję lub przez organ nadzorczy i następnie zatwierdzone przez Komisję) pozostaną jedną z alternatyw, a istniejące zestawy standardowych klauzul nadal będą obowiązywać.

Dopuszczalne będzie także korzystanie z innych zabezpieczeń, np. wiążących reguł korporacyjnych (BCR) oraz wiążących i egzekwowalnych instrumentów prawnych pomiędzy organami publicznymi.

Co istotne, przekazywanie danych do państw trzecich będzie dopuszczalne w przypadku zastosowania zatwierdzonego kodeksu postępowania (na podstawie art. 40) lub zatwierdzonego mechanizmu certyfikacji (art. 42), pod warunkiem podjęcia wiążących i egzekwowalnych zobowiązań przez administratora danych lub podmiot przetwarzający w państwie trzecim w zakresie stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą. Istnieją także przepisy uwzględniające wykorzystywanie zabezpieczeń *ad hoc* pod warunkiem autoryzacji przez właściwe organy nadzorcze.

W zakresie wiążących reguł korporacyjnych, RODO uwzględnia w przepisach aktualne wymogi stawiane w odniesieniu do nich administratorom i podmiotom przetwarzającym dane. Reguły będą nadal wymagać zatwierdzenia przez właściwe organy nadzorcze, ale będą podlegać ocenie zgodnie z mechanizmem spójności. Będzie to użyteczne w tych państwach członkowskich, które nadal nie mogą stosować wiążących reguł korporacyjnych.

Istnieją nadal pewne wyjątki pozwalające na przekazywanie danych osobowych tylko w ograniczonych przypadkach, które są podobne do aktualnie istniejących wyjątków i obejmują: wyraźną zgodę, niezbędność do wykonania umowy, przypadki, gdy przekazanie jest niezbędne ze względu na ważny interes publiczny, roszczenia prawne, żywotne interesy, a także dane z rejestrów publicznych. Istnieje także nowy (ograniczony) wyjątek obejmujący jednorazowe przekazywanie danych dotyczących ograniczonej liczby osób w przypadku, gdy jest to konieczne w związku z ważnym, prawnie uzasadnionym interesem administratora (który nie może być podrzędny w stosunku do praw i interesów osób, których dane dotyczą) oraz w przypadku, gdy administrator dokonał oceny (i dokumentacji) wszystkich okoliczności przedmiotowego przekazania danych i doszedł do wniosku, że istnieje odpowiedni poziom ochrony. Podmiot odbierający dane jest zobowiązany powiadomić organ nadzorczy i osoby, których dane dotyczą, o przypadkach stosowania wyżej wspomnianego wyjątku.

Wreszcie, zgodnie z oczekiwaniami, na podstawie RODO, niezgodne z prawem jest przekazywanie danych osobowych poza terytorium EOG na podstawie wymogów prawnych ze strony państw trzecich, chyba że wymogi te są oparte na międzynarodowych umowach, lub gdy istnieją inne dopuszczalne podstawy dla przekazywania danych. Wielka Brytania nie ratyfikowała tego postanowienia.

Gdzie mogę to znaleźć?
art. 40-45, motywy 78-91

Powoływanie organów nadzorczych

Na pierwszy rzut oka

- Krajowe organy ochrony danych nadal będą istnieć.
- Muszą one współpracować między sobą, a także z Komisją Europejską w celu monitorowania stosowania RODO.
- Muszą one działać w sposób niezależny.
- Funkcjonariusze organów nadzorczych muszą być powoływani w sposób przejrzysty, a także muszą być wykwalifikowani w dziedzinie ochrony danych.

Co trzeba zrobić

Nie ma potrzeby podejmowania żadnych działań, (chyba że są Państwo członkami istniejącego organu ochrony danych lub jego kadry pracowniczej!).

Komentarz

Krajowe organy ochrony danych (organy nadzorcze) nadal będą funkcjonować. Ich zadaniem będzie monitorowanie stosowania przepisów RODO w celu ochrony podstawowych praw w odniesieniu do przetwarzania danych, oraz wspierania swobodnego przepływu danych osobowych w obrębie UE.

Są one zobowiązane do współpracy między sobą oraz z Komisją Europejską w celu wspierania spójnego stosowania przepisów RODO.

Państwa takie, jak Niemcy, mogą nadal mieć więcej, niż jeden organ nadzorczy, ale jeden z nich musi zostać mianowany przedstawicielem organów krajowych w EROD.

Komisja musi być powiadamiana o krajowych przepisach prawa w zakresie ustanawiania i powoływania organów nadzorczych.

Organy nadzorcze mają działać w sposób całkowicie niezależny (i podlegać inspekcji finansowej oraz nadzorowi sądowniczemu). Członkowie organów nadzorczych mają nie poddawać się wpływom zewnętrznym i nie przyjmować od nikogo poleceń (oraz nie ubiegać się o nie). Nie wolno im podejmować działań, które są niezgodne z ich zakresem obowiązków, ani też angażować się w działalność niezgodną z zajmowanym stanowiskiem bez względu na to, czy czynności te są odpłatne, czy też nie.

Państwa członkowskie muszą zapewnić swoim organom nadzorczym odpowiednie zasoby ludzkie, techniczne, finansowe i inne, jakie okażą się konieczne w celu skutecznej realizacji ich zadań i korzystania z przyznanych im uprawnień.

Każdy organ nadzorczy sam wybiera swoje kadry i posiada nad nimi wyłączną zwierzchność. Budżet organu nadzorczego musi być znany publicznie i definiowany osobno nawet, jeśli stanowi element budżetu narodowego.

Przepisy prawa krajowego konstytuują organy nadzorcze, ustanawiają zasady działania ich członków, ich kwalifikacje i warunki wyboru. Kadencja członków organów nadzorczych nie może być krótsza, niż cztery lata i może być przedłużana przez władze państwa członkowskiego. Obowiązki członków tych organów w zakresie niezależności, o których mowa powyżej, muszą być przewidziane w przepisach prawa krajowego. Członkowie organów nadzorczych oraz ich kadra pracownicza są związani obowiązkiem *„tajemnicy zawodowej”* zarówno w czasie pełnienia obowiązków, jak i poza służbą.

Powyższe przepisy dotyczące ustanawiania organów nadzorczych stanowią rozwinięcie art. 28 starej dyrektywy w sprawie ochrony danych. W nowych zasadach nie ma niczego szczególnie nadzwyczajnego. Niektóre punkty są jednak warte wzmianki: np. specyfika kadencji, nacisk na niezależność, konieczność zapewnienia odpowiednich środków dla każdego organu nadzorczego, a także wymóg, według którego *„Każdy członek [organu nadzorczego] musi posiadać kwalifikacje, doświadczenie i umiejętności – w szczególności w dziedzinie ochrony danych osobowych – potrzebne do wypełniania swoich obowiązków i wykonywania swoich uprawnień.”*

Można spodziewać się dyskusji na temat tego, czy organy nadzorcze są odpowiednio finansowane, w szczególności w takich przypadkach, jak w Wielkiej Brytanii, gdzie nie będzie już tradycyjnej możliwości finansowania z opłat rejestracyjnych i notyfikacyjnych.

Gdzie mogę to znaleźć?
motywy 117-123, rozdział VI sekcja 1, art. 51-54

Właściwość, zadania i uprawnienia

Na pierwszy rzut oka

- Organy nadzorcze otrzymują określone kompetencje do podejmowania działań na własnym terytorium.
- Wiodący organ nadzorczy posiada kompetencje w sprawach transgranicznych (więcej informacji w części poświęconej współpracy i spójności pomiędzy organami nadzorczymi).
- Organy nadzorcze otrzymują szerokie uprawnienia i zadania.

Co trzeba zrobić

- Należy zapoznać się z uprawnieniami i zadaniami organów nadzorczych.
- W przypadku, gdy podejmują Państwo działania w zakresie transgranicznego przetwarzania danych, należy zapoznać się z systemem wiodących organów nadzorczych (więcej informacji na ten temat znajduje się w części poświęconej współpracy i spójności pomiędzy organami nadzorczymi)
- Mogą Państwo także rozważyć wdrożenie rozwiązań zgodnych z zatwierdzonym kodeksem postępowania lub mechanizmem certyfikacji, który wymaga aprobaty organu nadzorczego.

Właściwość

Organy nadzorcze (znane także potocznie jako „organy ochrony danych") otrzymują właściwość *„do wypełniania zadań i wykonywania powierzonych im uprawnień"* zgodnie z postanowieniami RODO i na ich rodzimym terytorium. Zgodnie z Motywem 122, wyżej wspomniana właściwość obejmuje *„przetwarzanie mające wpływ na osoby, których dane dotyczą, na tym terytorium lub przetwarzanie dokonywane przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli zwracają się oni do osób, których dane dotyczą, mających miejsce zamieszkania na tym terytorium"*.

W przypadku, gdy podstawą prawną przetwarzania, czy to przez podmiot prywatny, czy też organ władzy publicznej, jest obowiązek prawny bądź wykonywanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, dany organ władzy uznaje się za właściwy, a transgraniczny system wiodących organów nadzorczych nie ma zastosowania. Powyższe sformułowania są dość trudne do zrozumienia, ale Motyw 128 stwierdza, że organ nadzorczy posiada wyłączną jurysdykcję zarówno nad władzami publicznymi, jak i podmiotami prywatnymi działającymi w interesie publicznym, jeśli podmioty te posiadają jednostki organizacyjne na terytorium właściwości przedmiotowego organu. Jednakże nie jest oczywiste, czy uwzględnia to sytuacje, w których istnieje wiele jednostek organizacyjnych i jest sposobem na wykluczenie modelu pojedynczej instytucji lub czy też daje to wyłączną jurysdykcję lokalnemu organowi nadzorczemu nawet, jeśli przetwarzanie ma miejsce w innym państwie UE. Może to mieć szerokie zastosowanie w sektorze prywatnym, np. na rynku instytucji finansowych prowadzących działania przeciwdziałające praniu brudnych pieniędzy w odniesieniu do klientów zlokalizowanych w innym państwie członkowskim UE.

Organy nadzorcze nie mają właściwości nadrzędnej w stosunku do sądów działających w ramach sprawowania wymiaru sprawiedliwości. Słowo „sąd" nie zostało zdefiniowane i nie jest zupełnie jasne jak daleko w hierarchii sądowniczej sięgać będzie ta zasada.

System wiodących organów nadzorczych został powołany w celu radzenia sobie z kwestiami przetwarzania danych w kontekście transgranicznym (więcej informacji znajduje się w części poświęconej współpracy i spójności pomiędzy organami nadzorczymi, która dodatkowo objaśnia to skomplikowane pojęcie).

Zadania

Przygotowana została kompleksowa lista zadań wyznaczonych organom nadzorczym, której zapis znajduje się w art. 57 RODO. Nie ma potrzeby przywoływania jej w całości, ponieważ ostatnią pozycją jest *„wypełnianie innych zadań związanych z ochroną danych osobowych"*. Organy nadzorcze muszą zatem robić wszystko, co w uzasadniony sposób wchodzi w zakres *„ochrony danych osobowych"*.

Warto przyjrzeć się w sposób szczególny niektórym zadaniom. Organy nadzorcze mają za zadanie monitorować i egzekwować *„stosowanie"* przepisów RODO, a także promować wiedzę wśród społeczeństwa, administratorów i podmiotów przetwarzających dane.

Ich zadaniem jest doradzanie rządom i parlamentom w zakresie projektów nowych ustaw.

Pomaganie osobom, których dane dotyczą, rozpatrywanie i badanie skarg składanych przez osoby lub organy przedstawicielskie, prowadzenie dochodzeń, a w szczególności współpraca z innymi organami nadzorczymi to zadania wymienione ze szczególnym naciskiem, podobnie jak monitorowanie rozwoju praktyk technicznych i handlowych w zakresie technologii informacyjnej.

Organy nadzorcze mają także promować rozwój kodeksów postępowania i systemów certyfikacji, jak również *„opracowywać i publikować kryteria akredytacji"* w odniesieniu do podmiotów certyfikujących oraz monitorujących kodeksy postępowania.

Organy nadzorcze nie mogą pobierać od osób, których dane dotyczą, ani też od inspektorów ochrony danych, opłat za swoje usługi, jednakże RODO nie zawiera przepisów w zakresie tego, czy od administratorów lub podmiotów przetwarzających dane mogą być pobierane opłaty z tytułu usług świadczonych na ich rzecz przez organy nadzorcze.

Uprawnienia

Art. 58 RODO zawiera wykaz uprawnień organów nadzorczych, który może zostać rozszerzony przez państwa członkowskie według ich uznania. Wiele spośród tych uprawnień odpowiada zadaniom wyszczególnionym w art. 57 i nie ma potrzeby ich ponownego przywoływania.

Warto jednak wspomnieć o prawie do: nakazywania administratorowi lub podmiotowi przetwarzającemu przekazania informacji, prowadzenia postępowań w formie audytów, dostępu do pomieszczeń i danych, wydawania ostrzeżeń i udzielania upomnień oraz nakładania kar pieniężnych; jak również do nakazywania administratorom i podmiotom przetwarzającym dane przestrzegania przepisów RODO i praw osób, których dane dotyczą; zakazywania przetwarzania danych i przekazywania danych poza granice UE; zatwierdzania standardowych klauzul umownych i wiążących reguł korporacyjnych. Wykonywanie uprawnień przez organ nadzorczy musi podlegać odpowiednim zabezpieczeniom i umożliwiać odwołanie przed sądem.

Państwa członkowskie muszą zapewnić swoim organom nadzorczym prawo do zgłaszania spraw do organów wymiaru sprawiedliwości „w stosownych przypadkach do wszczęcia lub do uczestniczenia w inny sposób w postępowaniu sądowym w celu wyegzekwowania stosowania przepisów niniejszego rozporządzenia". Przypuszczalnie istniejący rozdział uprawnień zostanie utrzymany zgodnie z prawem i procedurami krajowymi.

Wreszcie, organy nadzorcze są zobowiązane do składania rocznych raportów. Podsumowując, właściwość, uprawnienia i zadania organów nadzorczych stanowią kompleksowy katalog tego, co organ nadzorczy musi, oraz może, robić. Jest to w dużej mierze przewidywalna konsolidacja istniejących praktyk z uwzględnieniem pewnych nowych rozwiązań stosowanych w poszczególnych państwach członkowskich.

Gdzie mogę to znaleźć?
motywy 117-123, Opinia Grupy Roboczej WP 244, rozdział VI sekcja 2, art. 55-59

Współpraca i spójność pomiędzy organami nadzorczymi

Na pierwszy rzut oka

W przypadku transgranicznego przetwarzania danych w UE, Komisja Europejska zaproponowała model pojedynczej instytucji, w ramach którego organ nadzorczy właściwy dla głównej jednostki organizacyjnej administratora danych byłby jedynym organem w zakresie monitorowania i zapewniania zgodności z przepisami prawa UE. W obliczu silnego sprzeciwu rozwiązanie to zostało osłabione.

W obecnym kształcie będzie funkcjonować wiodący organ nadzorczy dla spraw, w których istnieje wiele jednostek organizacyjnych lub w których odbywa się transgraniczne przetwarzanie na terytorium UE, który będzie organem nadzorczym właściwym dla głównej jednostki organizacyjnej, ale organy nadzorcze w innych państwach, w których ten administrator posiada jednostki organizacyjne, lub w których osoby, których dane dotyczą znajdują się pod znacznym wpływem działań tego administratora, lub też organy nadzorcze, do których złożona została skarga, mogą być zaangażowane w niektóre sprawy, a wiodący organ nadzorczy jest zobowiązany z tymi organami współpracować. Organy niemające statusu wiodącego organu nadzorczego także mogą zajmować się sprawami o charakterze czysto lokalnym, w które zaangażowany jest transgraniczny administrator danych.

Co trzeba zrobić

- W przypadku, gdy podejmują Państwo działania w zakresie tylko jednego państwa członkowskiego - (co nadal ma zastosowanie do większości przedsiębiorstw), system wiodących organów nadzorczych nie ma zastosowania, a mechanizm sporny może na Państwa wpływać wyłącznie w przypadku, gdy jakiś proponowany kodeks postępowania lub mechanizm certyfikacji zostanie opóźniony lub zakwestionowany przez EROD.
- W przypadku, gdy podejmują Państwo działania w dwóch lub więcej państwach członkowskich, należy sprawdzić, który organ jest dla Państwa wiodącym organem nadzorczym, a następnie nawiązać z nim kontakt np. poprzez skorzystanie ze szkolenia i wytycznych, jakie organ ten oferuje.

Komentarz

Właściwość Wiodących Organów Nadzorczych

W przypadku, gdy administrator lub podmiot przetwarzający dane zajmuje się transgranicznym przetwarzaniem danych osobowych, albo za pomocą sieci jednostek organizacyjnych na terytorium UE albo za pomocą tylko jednej jednostki organizacyjnej, organ nadzorczy właściwy dla głównej lub jedynej jednostki organizacyjnej działa w charakterze wiodącego organu nadzorczego w odniesieniu do przedmiotowego przetwarzania.

Grupa Robocza przyjęła wytyczne na temat identyfikowania wiodącego organu nadzorczego. Jeżeli organizacja ma wiele jednostek organizacyjnych, wiodący organ ochrony danych ustala się na podstawie tego gdzie zapadają decyzje dotyczące celów przetwarzania i sposobów przetwarzania – przy czym może to być państwo siedziby organu zarządzającego administratora, jeżeli natomiast decyzje są podejmowane w innej jednostce organizacyjnej, organem wiodącym jest organ właściwy dla tej jednostki organizacyjnej. W wytycznych dostrzeżono, że w niektórych sytuacjach organem wiodącym może być więcej niż jeden organ, np. w przypadku międzynarodowych korporacji posiadających kilka oddzielnych centrów decyzyjnych, w różnych krajach, dla różnych czynności przetwarzania.

W odniesieniu do współadministratorów, zgodnie z wytycznymi Grupy Roboczej, aby skorzystać z dobrodziejstwa mechanizmu kompleksowej współpracy (eng. *one-stop-shop*) współadministratorzy powinni wyznaczyć jedną jednostkę organizacyjną, która będzie władna podejmować decyzje co do przetwarzania przez wszystkich współadministratorów. W praktyce jednak, przekazanie jednej jednostce organizacyjnej mocy podejmowania decyzji w powyższym znaczeniu może okazać się trudne, co może uczynić koncepcję organów wiodących teoretyczną.

Podobnie w przypadku podmiotów przetwarzających świadczących usługi na rzecz wielu administratorów – oni również nie skorzystają z mechanizmu kompleksowej współpracy z uwagi na to, że dla każdego administratora właściwy będzie inny organ wiodący.

W wytycznych podkreśla się, że RODO nie zezwala na „forum shopping" – muszą istnieć efektywne i rzeczywiste czynności zarządzania w państwie członkowskim wybranym, jako główna jednostka organizacyjna administratora. Administratorzy powinni być w stanie wykazać przed organami nadzorczymi gdzie są faktycznie podejmowane i egzekwowane decyzje w przedmiocie przetwarzania, z uwagi na to, że mogą być zobowiązani do udowodnienia ich stanowiska w tym zakresie. W wytycznych podkreśla się, że administratorzy bez jednostki organizacyjnej na terytorium UE nie mogą odnosić korzyści z tytułu „mechanizmu kompleksowej współpracy" – muszą natomiast w państwach, w których prowadzą działalność wyznaczyć do kontaktu z organami nadzorczymi swoich przedstawicieli.

Krajowy organ nadzorczy nadal może wykonywać swoje uprawnienia w przypadku złożenia skargi lub wykrycia naruszenia na jego terytorium i kiedy przedmiot skargi lub naruszenia odnosi się wyłącznie do jednostki organizacyjnej na tym terytorium, lub wywiera znaczny wpływ na osoby, których dane dotyczą na terytorium tego państwa. EROD może wydawać wytyczne dotyczące tego, co oznacza sformułowanie „*znaczny*" wpływ na osoby, których dane dotyczą na terytorium więcej niż jednego państwa członkowskiego. Wytyczne Grupy Roboczej zawierają interpretację pojęcia "*znacznego wpływu na osoby, których dane dotyczą*".

Tego typu lokalne przypadki muszą być zgłaszane wiodącemu organowi nadzorczemu, który w terminie trzech tygodni musi podjąć decyzję o ewentualnej interwencji (uwzględniając to, czy w innym państwie istnieje jednostka organizacyjna), a następnie skorzystać z procedury współpracy. Organy niemające statusu wiodącego organu nadzorczego mogą sugerować wiodącemu organowi nadzorczemu podejmowanie określonych decyzji.

W przypadku, gdy wiodący organ nadzorczy postanowi nie interweniować, lokalny organ nadzorczy przejmuje sprawę, w razie potrzeby korzystając z uprawnień w zakresie wzajemnej pomocy i wspólnego postępowania.

Procedura współpracy

Wiodący organ nadzorczy jest zobowiązany współpracować z innymi organami nadzorczymi „których sprawa dotyczy" w danej sprawie. Organy te są zobowiązane do wzajemnej wymiany informacji i muszą działać w kierunku osiągnięcia porozumienia.

Wiodący organ nadzorczy jest zobowiązany dostarczać informacji innym organom nadzorczym, może także ubiegać się o wzajemną pomoc ze strony pozostałych organów oraz prowadzić z nimi wspólne postępowania na ich terytorium. Wiodący organ nadzorczy musi bez zbędnej zwłoki przekazać projekt decyzji pozostałym zaangażowanym organom, które mogą wyrazić sprzeciw w terminie czterech tygodni. Proces składania projektu może zostać przeprowadzony ponownie z dwutygodniowym terminem na wnoszenie sprzeciwów. W przypadku, gdy wiodący organ nadzorczy postanowi nie postępować zgodnie ze stanowiskiem pozostałych zaangażowanych organów, musi poddać się procedurze spójności nadzorowanej przez EROD.

Istnieją szczegółowe zasady dotyczące tego, który organ nadzorczy powinien podjąć formalną decyzję i powiadomić administratora danych, jednak wiodący organ nadzorczy jest zobowiązany zapewnić, że zgodnie z formalną decyzją, administrator danych podejmie działania zmierzające w kierunku uzyskania zgodności z przepisami w odniesieniu do wszystkich swoich jednostek organizacyjnych.

W wyjątkowych sytuacjach wiodący organ nadzorczy może podjąć pilne, tymczasowe działania przed zakończeniem procesu spójności.

System wiodących organów nadzorczych ma kilka widocznych wad i może zostać osłabiony w przypadku, gdy organy nieposiadające statusu wiodącego organu nadzorczego są w stanie przypisać sobie właściwość na podstawie tego, że osoby, których dane dotyczą, a które zamieszkują na ich terytorium, znajdują się pod znacznym wpływem przetwarzania przez administratora danych, którego główna jednostka organizacyjna znajduje się w innym miejscu. Zatem powodzenie wiodącego organu nadzorczego będzie w dużej mierze zależeć od konsensusu i dobrej woli pomiędzy organami nadzorczymi.

Wzajemna Pomoc, Wspólne Operacje i Spójność

Organy nadzorcze są zobowiązane do udzielania sobie wzajemnej pomocy w postaci dostarczania informacji lub prowadzenia *„uprzednich konsultacji oraz przeprowadzenia kontroli i postępowań*

wyjaśniających". Komisja Europejska może określić formy i procedury wzajemnej pomocy.

Organy nadzorcze mogą prowadzić wspólne postępowania i działania w zakresie egzekwowania prawa. Organ nadzorczy ma także prawo do uczestnictwa we wspomnianych operacjach w przypadku, gdy administrator danych posiada jednostkę organizacyjną na jego terytorium lub gdy operacje przetwarzania mogą istotnie wpłynąć na znaczną liczbę osób, których dane dotyczą. Jeśli miejscowe prawo na to pozwala, pierwotny organ nadzorczy może przekazać formalne uprawnienia do prowadzenia postepowań specjalnie oddelegowanym pracownikom. Organy nadzorcze prowadziły już wspólne operacje na mocy istniejących przepisów prawa, tak więc RODO w praktyce prawdopodobnie spowoduje tylko rozwinięcie i wzmocnienie tych mechanizmów.

W przypadku, gdy organy nadzorcze podejmują pewne formalne kroki lub też wyrażają przeciwne zdanie lub wnioskują o podjęcie działań przez inny organ nadzorczy, zapisy RODO przewidują zastosowanie mechanizmu spójności i rozwiązywania sporów. W swoich wytycznych Grupa Robocza kładzie nacisk na kwestię współpracy między wiodącym organem nadzorczym a pozostałymi organami, aby zapewnić, że postępowanie w sprawie i jej rozstrzygnięcie będą satysfakcjonujące dla każdego z organów podkreślając jednocześnie, że formalny mechanizm spójności należy powołać tylko wtedy, gdy współpraca nie przyniesie rezultatu wzajemnie akceptowalnego przez wszystkie zainteresowane organy.

EROD wydaje opinie dotyczące różnych propozycji ze strony organów nadzorczych, w tym w zakresie zatwierdzania wiążących reguł korporacyjnych, kryteriów certyfikacji i kodeksów postępowania. W przypadku, gdy organ nadzorczy nie zgodzi się z opinią EROD, sprawa zostaje poddana procedurze rozwiązywania sporów.

Procedura ta ma zastosowanie także w przypadku sporów pomiędzy wiodącym organem nadzorczym a innymi zaangażowanymi organami nadzorczymi. W każdym z tych przypadków, EROD podejmuje wiążącą decyzję większością dwóch trzecich głosów. W przypadku, gdy wyżej wspomniana większość nie zostanie osiągnięta, do podjęcia decyzji wystarczająca jest większość zwykła. Organy nadzorcze, których sprawa dotyczy, są zobowiązane do przestrzegania wyżej wspomnianego rozstrzygnięcia, a wszelkie decyzje formalne muszą być podejmowane w zgodności z decyzją EROD.

Gdzie mogę to znaleźć?
motywy 124-138 i rozdział VII, sekcje 1 i 2

Europejska Rada Ochrony Danych

Na pierwszy rzut oka

- Dawna Grupa Robocza, w której skład wchodziły krajowe organy nadzorcze państw UE, Europejski Inspektor Ochrony Danych („EIOD"), a także Komisja Europejska, zostały przekształcone w Europejską Radę Ochrony Danych, która charakteryzuje się podobnym składem, lecz posiada niezależny sekretariat.
- EROD posiada status organu UE posiadającego osobowość prawną i szerokie uprawnienia pozwalające na rozstrzyganie sporów pomiędzy krajowymi organami nadzorczymi, doradztwo i wydawanie wytycznych, a także zatwierdzanie kodeksów postępowania oraz certyfikacji o unijnym zasięgu.

Co trzeba zrobić

Nie potrzeba żadnych natychmiastowych działań - chyba, że są Państwo członkami istniejącego krajowego organu nadzorczego.

Jednakże EROD będzie wywierać znaczny wpływ na unijne prawo i praktyki w zakresie ochrony danych i zaleca się podjęcie działań mających wpłynąć na decyzje tej instytucji.

Komentarz

Grupa Robocza, która została ustanowiona na mocy dyrektywy w sprawie ochrony danych i która składa się z przedstawicieli organów nadzorczych państw członkowskich UE oraz przedstawicieli Komisji i EIOD, zostanie zniesiona na mocy przepisów RODO. Zostanie ona zastąpiona przez EROD, która podobnie będzie składać się z szefów krajowych organów nadzorczych (lub ich przedstawicieli) oraz EIOD.

Przedstawiciel Komisji w EROD nie posiada prawa głosu, a w państwach (takich, jak np. Niemcy) posiadających więcej, niż jeden organ nadzorczy, wspólny przedstawiciel musi zostać powołany na gruncie prawa krajowego. W sprawach dotyczących rozwiązywania sporów, kiedy konieczne jest podjęcie wiążącej decyzji, uprawnienia EIOD do głosowania są ograniczone do okoliczności, w których zasady wynikające z danej sprawy miałyby zastosowanie do instytucji Unii.

Pozycja EROD jest znacznie silniejsza niż dotychczasowego organu. Nie jest to jedynie komisja doradcza, ale niezależny organ Unii z własną osobowością prawną.

Rada jest formalnie reprezentowana przez przewodniczącego, który pełni główną rolę w organizowaniu prac EROD, w szczególności w zakresie zarządzania procedurą rozstrzygania sporów pomiędzy krajowymi organami nadzorczymi. Przewodniczącego i dwóch wiceprzewodniczących wybiera się spośród członków EROD na kadencję pięciu lat, która może zostać powtórzona jeden raz.

EROD zazwyczaj podejmuje decyzje zwykłą większością głosów, jednakże reguły procedowania i wydawania wiążących decyzji (w pierwszej instancji) wymagają większości dwóch trzecich głosów.

EROD musi uchwalić własne reguły procedowania oraz samodzielnie zorganizować swoje prace. Podkreśla się niezależność EROD. Istnieje pośrednia sugestia, jakoby Komisja Europejska wywierała w przeszłości zbyt duży wpływ na Grupę Roboczą próbując skonsolidować uprawnienia w tym zakresie.

Sekretarzem dawnej Grupy Roboczej Art. 29 był urzędnik Komisji. EROD będzie mieć swój własny sekretariat zapewniony przez EIOD, który będzie jednak wykonywać swoje zadania wyłącznie pod kierunkiem przewodniczącego Europejskiej Rady Ochrony Danych.

EROD otrzymała długą i szczegółową listę zadań, jednak jej główną rolą jest praca na rzecz spójnego stosowania przepisów RODO w całej UE. EROD doradza Komisji, w szczególności w zakresie ochrony zapewnianej przez państwa trzecie oraz organizacje międzynarodowe, a także ma za zadanie promować współpracę pomiędzy krajowymi organami nadzorczymi. Ponadto, EROD wydaje wytyczne, rekomendacje i wykazy najlepszych praktyk: na przykład w przypadkach, gdy naruszenie ochrony danych może „powodować wysokie ryzyko naruszenia praw lub wolności" osób fizycznych, lub też w zakresie wymogów stawianych wiążącym regułom korporacyjnym. Ma ponadto za zadanie promować kodeksy postępowania i mechanizmy certyfikacji, co ma pomagać administratorom i podmiotom przetwarzającym dane w wykazywaniu zgodności z RODO.

Wiele spośród wyżej wymienionych zadań stanowi rozwinięcie lub sformalizowanie działalności Grupy Roboczej, jednakże poglądy i działalność EROD będą miały większe znaczenie i moc prawną.

Najważniejszą z nowych ról EROD jest łagodzenie i rozstrzyganie sporów pomiędzy krajowymi organami nadzorczymi. Więcej informacji na ten temat znajduje się w części poświęconej właściwości, zadaniom i uprawnieniom. Dawna Grupa Robocza była często krytykowana za zbyt pochopne podejmowanie decyzji. EROD będzie musiała skonsultować się z zainteresowanymi stronami *„w stosownych przypadkach"*. Jest to istotna korzyść dla osób, na których opinie, wytyczne, wskazówki i proponowane najlepsze praktyki mogły wywierać negatywne skutki.

Dyskusje prowadzone przez EROD mają być *„poufne, jeżeli taką konieczność stwierdzi Rada zgodnie ze swoim regulaminem wewnętrznym"*. Powyższe sugeruje, że spotkania i dyskusje będą, co do zasady, jawne o ile nie zostanie postanowione inaczej.

Wreszcie, EROD jest zobowiązana do przygotowywania rocznego sprawozdania.

Gdzie mogę to znaleźć?
motywy 139 i 140 oraz rozdział VII, sekcja 3

Środki prawne i odpowiedzialność

Na pierwszy rzut oka

- Osoby fizyczne mają następujące prawa (względem administratorów i podmiotów przetwarzających dane):
  - prawo do wniesienia skargi do organu nadzorczego w przypadku, gdy ich dane były przetwarzane w sposób niezgodny z przepisami RODO;
  - prawo do skutecznego środka ochrony prawnej przed sądem w przypadku, gdy właściwy organ nadzorczy nie będzie w stanie odpowiednio rozpatrzyć skargi;
  - prawo do skutecznego środka ochrony prawnej przed sądem w odniesieniu do określonego administratora lub podmiotu przetwarzającego dane; oraz
  - prawo do odszkodowania (albo zadośćuczynienia) ze strony administratora danych lub podmiotu przetwarzającego dane w odniesieniu do szkód majątkowych i niemajątkowych będących następstwem naruszenia przepisów RODO.
- Zarówno osoby fizyczne, jak i osoby prawne są uprawnione do wniesienia odwołania do sądu krajowego od wiążącej decyzji wydanej przez organ nadzorczy, której są adresatem.
- Osoby fizyczne są uprawnione do zgłaszania roszczeń z tytułu szkody o charakterze niemajątkowym oprócz roszczeń odszkodowawczych z tytułu szkody majątkowej. Potencjalna możliwość wnoszenia pozwów zbiorowych jest dodatkowo zaakcentowana.

Środki ochrony prawnej oraz odpowiedzialność odszkodowawcza rozciągają się zarówno na administratorów danych, jak i podmioty przetwarzające dane, którzy naruszają postanowienia RODO.

Co trzeba zrobić

- Administratorzy i podmioty przetwarzające dane powinni zapewnić, że umowy powierzenia przetwarzania danych oraz umowy dotyczące zarządzania kontraktami w sposób jasny określają zakres obowiązków podmiotu przetwarzającego dane, a także powinni uzgodnić odpowiednie mechanizmy rozstrzygania sporów w zakresie odpowiedzialności w celu ułatwienia rozwiązywania sporów o charakterze odszkodowawczym.
- Administratorzy i podmioty przetwarzające dane powinni powiadamiać innych administratorów lub podmioty przetwarzające dane, zaangażowanych w te same operacje przetwarzania, o wszelkich naruszeniach zgodności oraz wszelkich skargach i roszczeniach wysuwanych przez osoby, których dane dotyczą.
- Współadministratorzy danych oraz administratorzy prowadzący wspólnie procesy przetwarzania danych powinni uzgodnić zakresy swoich obowiązków z punktu widzenia zgodności z przepisami o ochronie danych, a także zakresy odpowiedzialności z tytułu naruszenia ochrony danych oraz mechanizmy rozwiązywania sporów w przedmiocie wspomnianej odpowiedzialności w celu ułatwienia rozwiązywania sporów o charakterze odszkodowawczym.

Skargi kierowane do organów nadzorczych

Prawa osób, których dane dotyczą w zakresie składania skarg do organów nadzorczych zostały nieznacznie wzmocnione w porównaniu do dyrektywy w sprawie ochrony danych. Wspomniana dyrektywa zobowiązuje organy nadzorcze do rozpatrywania skarg składanych przez osoby, których dane dotyczą, których przedmiotem jest sprawdzenie zgodności z prawem przetwarzania danych, a także do informowania osób, których dane dotyczą o przeprowadzeniu czynności sprawdzających.

Na mocy RODO osoby, których dane dotyczą, i których dane osobowe są przetwarzane w sposób, który nie jest zgodny z postanowieniami RODO, mają wyraźne prawo do skierowania do organu nadzorczego skargi, a organ nadzorczy jest zobowiązany powiadomić osoby, których dane dotyczą, o postępach i wyniku postępowania.

Środki ochrony prawnej przeciwko decyzjom organów nadzorczych

Zarówno osoby, których dane dotyczą, jak i inne osoby, są uprawnione do korzystania ze skutecznych środków ochrony prawnej w odniesieniu do pewnych działań i decyzji organów nadzorczych.

- Każda osoba ma prawo do skutecznego środka ochrony prawnej w odniesieniu do prawnie wiążących decyzji ich dotyczących, podjętych przez organy nadzorcze.
- Osoby, których dane dotyczą mają prawo do skutecznego środka ochrony prawnej przed sądem w przypadku, gdy organ nadzorczy nie rozpatrzy skargi lub nie powiadomi osoby, której dane dotyczą, w ciągu trzech miesięcy o postępach lub efektach rozpatrywania skargi.

Motyw 143 wyjaśnia, że decyzje i działania, które mogą zostać podważone w sądzie obejmują wykonywanie przez organ nadzorczy uprawnień do prowadzenia postępowań wyjaśniających, uprawnień naprawczych i do wydawania zezwoleń, jak również oddalania lub odrzucania skarg. Wspomniane prawo nie obejmuje innych środków podejmowanych przez organy nadzorcze, które nie są prawnie wiążące, np. wydawanych opinii lub zalecień ze strony organów nadzorczych.

Środki ochrony prawnej przeciwko administratorom i podmiotom przetwarzającym dane

Osoby, których dane dotyczą, a których prawa zostały naruszone, są uprawnione do skutecznego środka ochrony prawnej wobec administratora danych lub podmiotu przetwarzającego dane, który odpowiada za domniemane naruszenie. Dyrektywa w sprawie ochrony danych zawiera podobne postanowienia dotyczące środków ochrony prawnej wobec administratorów danych, jednak nie w odniesieniu do podmiotów przetwarzających dane.

Odpowiedzialność odszkodowawcza

Każda osoba, która poniosła szkodę na skutek naruszenia przepisów RODO, jest uprawniona do odszkodowania ze strony administratora danych lub podmiotu przetwarzającego dane. Na mocy dyrektywy w sprawie ochrony danych odpowiedzialność odszkodowawcza jest ograniczona wyłącznie do administratorów.

Zasady odpowiedzialności pomiędzy administratorami a podmiotami przetwarzającymi dane przedstawiają się następująco:

- administratorzy danych odpowiadają za szkody powstałe na skutek przetwarzania danych w sposób niezgodny z postanowieniami RODO;
- podmioty przetwarzające dane odpowiadają wyłącznie za szkody powstałe na skutek przetwarzania danych z naruszeniem obowiązków nałożonych na te podmioty przez RODO, lub spowodowane przetwarzaniem danych, które wykracza poza zakres lub narusza instrukcje wydane przez administratora danych; oraz
- w celu zapewnienia skutecznego odszkodowania dla osób, których dane dotyczą, administratorzy i podmioty przetwarzające dane zaangażowane w te same operacje przetwarzania, i którzy są odpowiedzialni za jakiekolwiek wyrządzone szkody, będą każdorazowo pociągani do odpowiedzialności za całość wyrządzonych szkód. Jednakże, administratorowi danych lub podmiotowi przetwarzającemu dane, na którego spada odpowiedzialność odszkodowawcza na wyżej wspomnianej podstawie, przysługuje regres w stosunku do innych podmiotów w takiej części nałożonego odszkodowania, która odpowiada za ich udział w wyrządzonych szkodach.

Podczas, gdy postanowienia dyrektywy w sprawie ochrony danych odnoszą się wyłącznie do prawa do odszkodowania za *„szkody majątkowe”*, postanowienia RODO stanowią, że odszkodowania (zadośćuczynienia) można dochodzić z tytułu zarówno szkód o charakterze majątkowym, jak i niemajątkowym. To stwierdzenie jest spójne z aktualną angielską wykładnią pojęcia szkody dla celów rozpatrywania roszczeń odszkodowawczych na mocy dyrektywy w sprawie ochrony danych (patrz Google Inc. v Vidal-Hall & Others [2015] EWCA Civ 311).

Zgodnie z RODO administratorzy i podmioty przetwarzające dane są zwolnieni z odpowiedzialności prawnej, jeżeli *„szkoda w żadnym razie nie powstała z ich winy”*. To odstępstwo wydaje się mieć nieznacznie węższy zakres, niż odstępstwo, na które może się powoływać administrator danych na mocy dyrektywy w sprawie ochrony danych, który jest w stanie udowodnić, że *„nie jest odpowiedzialny za zdarzenie, które spowodowało szkodę*."

Reprezentowanie osób, których dane dotyczą

RODO nadaje osobom, których dane dotyczą, prawo do powoływania odpowiednio ukonstytuowanych organizacji przedstawicielskich dla celów składania skarg u organów nadzorczych w imieniu wspomnianych osób oraz do ubiegania się w ich imieniu o środki ochrony prawnej w odniesieniu do decyzji organów nadzorczych lub wobec administratorów lub podmiotów przetwarzających dane. Wspomniane postanowienia dotyczą organizacji przedstawicielskich, które:

- nie są podmiotami, organizacjami lub zrzeszeniami prowadzącymi działalność zarobkową;
- zostały należycie ustanowione zgodnie z prawem państwa członkowskiego;
- których cele statutowe leżą w interesie publicznym; oraz
- aktywnie działają na polu ochrony danych

Osoby, których dane dotyczą, mogą także upoważnić wyżej wspomniane organizacje do wykonywania w ich imieniu uprawnień w zakresie dochodzenia odszkodowania od administratorów lub podmiotów przetwarzających dane, o ile jest to dozwolone na gruncie prawa danego państwa członkowskiego.

Jeżeli prawo państwa członkowskiego na to pozwala, wspomniane organizacje reprezentujące osoby, których dane dotyczą mogą, niezależnie od upoważnienia ze strony osób, których dane dotyczą, wnosić skargi do organów nadzorczych i ubiegać się o środki ochrony prawnej przeciwko decyzjom organów nadzorczych lub w stosunku do administratorów lub podmiotów przetwarzających dane.

Dyrektywa w sprawie ochrony danych nie zawiera przepisów, które odpowiadają wyżej opisanym postanowieniom.

Gdzie mogę to znaleźć?
art. 77-82, motywy 141-147

Administracyjne kary pieniężne

Na pierwszy rzut oka

- Organy nadzorcze są uprawnione do nakładania administracyjnych kar pieniężnych o znacznej wysokości na administratorów i podmioty przetwarzające dane.
- Kary pieniężne mogą być nakładane zamiast lub oprócz innych środków, które przysługują organom nadzorczym. Mogą być nakładane z tytułu szerokiego zakresu naruszeń, w tym o charakterze czysto proceduralnym.
- Administracyjne kary pieniężne mają charakter uznaniowy. Muszą być nakładane z uwzględnieniem okoliczności konkretnej sprawy i muszą być *„skuteczne, proporcjonalne i odstraszające”*.
- Rozróżnić można dwa poziomy administracyjnych kar pieniężnych:
  - Niektóre naruszenia podlegają administracyjnym karom pieniężnym w wysokości do 10 000 000 euro lub, w przypadku przedsiębiorstw, do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która kwota jest wyższa.
  - Inne naruszenia podlegają administracyjnym karom pieniężnym w wysokości do 20 000 000 euro lub, w przypadku przedsiębiorstw, do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego z poprzedniego roku obrotowego, w zależności od tego, która kwota jest wyższa.
- Państwa członkowskie mogą samodzielnie określić, czy, i w jakim zakresie, organy i podmioty publiczne powinny podlegać administracyjnym karom pieniężnym

Co trzeba zrobić

- Należy przeprowadzić analizę luk w zakresie przepisów RODO w celu zidentyfikowania obszarów najpoważniejszej niezgodności oraz ustalenia hierarchii czynności naprawczych, w szczególności w odniesieniu do operacji przetwarzania o wysokim poziomie ryzyka.
- Należy uaktualnić rejestry ryzyka.
- Ponadto, należy ocenić ryzyko wystąpienia odpowiedzialności w odniesieniu do istniejących umów z klientami, dostawcami oraz partnerami, w tym poprzez dokonanie oceny umownych ograniczeń odpowiedzialności i wyłączeń odpowiedzialności.
- Dodatkowo, zaleca się dokonanie przeglądu polis ubezpieczeniowych.

Informacje ogólne

Administracyjne kary pieniężne nie są stosowane automatycznie i powinny być nakładane z uwzględnieniem okoliczności konkretnego przypadku. Motyw 148 stwierdza, że w przypadku niewielkiego naruszenia, oraz w przypadku, gdy kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, zamiast kary można udzielić upomnienia.

Aktualnie istnieje duża rozbieżność pomiędzy państwami członkowskimi w zakresie nakładania kar pieniężnych przez organy nadzorcze. O ile przepisy RODO przewidują maksymalne wysokości kar pieniężnych i dają organom nadzorczym pewną swobodę w zakresie ich stosowania, Motyw 150 wskazuje, że w celu wspierania jednolitego stosowania tego środka można skorzystać z mechanizmu spójności.

Jednakże każde państwo członkowskie może samodzielnie ustalić zasady odnośnie do tego, czy i w jakim stopniu administracyjne kary pieniężne mogą być nakładane na organy publiczne i podmioty należycie ustanowione zgodnie z prawem danego państwa członkowskiego.

Maksymalne wysokości administracyjnych kar pieniężnych

Postanowienia RODO przewidują dwa zestawy maksymalnych progów dla administracyjnych kar pieniężnych, które mogą być nakładane za określone naruszenia.

W każdym przypadku, maksymalna wysokość kary jest wyrażona w euro lub, w przypadku przedsiębiorstw, jako procent całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która kwota jest wyższa. Motyw 150 potwierdza, że w powyższym kontekście „przedsiębiorstwo" należy rozumieć według definicji zawartej w art. 101 i 102 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE"), tj. ogólnie rzecz ujmując, jako podmioty prowadzące działalność gospodarczą.

Naruszenie następujących przepisów RODO podlega administracyjnej karze pieniężnej w wysokości do 20 000 000 euro lub, w przypadku przedsiębiorstw, do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która kwota jest wyższa:

- podstawowych zasad przetwarzania, w tym warunków zgody (art. 5, 6, 7 i 9);
- praw osób, których dane dotyczą (art. 12-22);
- transgranicznego przekazywania danych (art. 44-49);
- obowiązków wynikających z prawa państwa członkowskiego przyjętych na podstawie Rozdziału IX; oraz
- nieprzestrzegania poleceń wydanych przez organy nadzorcze (określonych w art. 58(2)) niezastosowanie się do postępowania prowadzonego przez organ nadzorczy na podstawie art. 58(1).

Pozostałe naruszenia podlegają administracyjnym karom pieniężnym w wysokości do 10 000 000 euro lub, w przypadku przedsiębiorstw, do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która kwota jest wyższa. Naruszenia podlegające wspomnianym maksymalnym karom pieniężnym obejmują naruszenie następujących obowiązków:

- obowiązku uzyskania zgody na przetwarzanie danych dotyczących dzieci (art. 8);
- obowiązków w zakresie wdrażania nowych środków technicznych i organizacyjnych w celu uwzględnienia ochrony danych w fazie projektowania i domyślnej ochrony danych (art. 25)
- obowiązków ustalenia zakresu swoich obowiązków dotyczących ochrony danych osobowych przez współadministratorów danych (art. 26);
- obowiązków nałożonych na administratorów danych i podmioty przetwarzające dane nieposiadających jednostki organizacyjnej na terytorium UE w zakresie wyznaczania przedstawicieli (art. 27);
- obowiązków nałożonych na administratorów danych w zakresie angażowania podmiotów przetwarzających dane (Art. 28);
- obowiązków nałożonych na podmioty przetwarzające dane w zakresie angażowania podwykonawców wyłącznie za uprzednią zgodą administratora danych oraz zgodnie z jego instrukcjami (art. 28-29);
- obowiązków w zakresie prowadzenia pisemnych rejestrów czynności przetwarzania (art. 30);
- obowiązków nałożonych na podmioty przetwarzające dane w zakresie współpracy z organami nadzorczymi (art 31);
- obowiązków w zakresie wdrażania środków technicznych i organizacyjnych (art. 32);
- obowiązków w zakresie zgłaszania naruszeń zgodnie z wymogami RODO (Art. 33-34);
- obowiązków w zakresie prowadzenia ocen skutków dla ochrony danych (Art. 35-36)
- obowiązków w zakresie powoływania inspektorów ochrony danych (Art. 37-39)
- obowiązków nakładanych na podmioty certyfikujące (art. 42-43); oraz
- obowiązków nakładanych na organy monitorujące w zakresie podejmowania działań w odpowiedzi na naruszenie kodeksów postępowania (art. 41).

W przypadkach, gdy te same lub powiązane ze sobą operacje przetwarzania danych są związane z naruszeniem więcej, niż jednego przepisu RODO, kary pieniężne nie mogą przekraczać kwoty przewidzianej za najcięższe naruszenie.

Czynniki do uwzględnienia

Art. 83(2) RODO zawiera wykaz czynników do uwzględnienia przy określaniu czy należy nałożyć administracyjną karę pieniężną, oraz przy decydowaniu o wysokości nałożonej kary. Powyższe obejmuje:

- charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
- umyślny lub nieumyślny charakter naruszenia;
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego
- wszelkie wcześniejsze naruszenia;
- stopień współpracy z organem nadzorczym;
- kategorie danych osobowych, których dotyczyło naruszenie;
- czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie do organu nadzorczego;
- historia wcześniejszych sankcji;
- stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz
- wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie w okolicznościach sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte pośrednio lub bezpośrednio straty

W przypadku, gdy kary pieniężne są nakładane na osoby niebędące przedsiębiorstwem, organ nadzorczy powinien, ustalając wysokość kary pieniężnej, uwzględnić także ogólny poziom zarobków w danym państwie członkowskim, jak również sytuację ekonomiczną danej osoby.

Gdzie mogę to znaleźć?
art. 83, motywy 148-152

Wyjątki i warunki szczególne

Na pierwszy rzut oka

Państwa członkowskie zachowają prawo do wprowadzania wyjątków, jeśli będzie to konieczne dla celów bezpieczeństwa narodowego, zapobiegania i wykrywania przestępczości, a także w pewnych innych sytuacjach. Zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej, każdy wyjątek musi być ustanawiany z poszanowaniem „*istoty*" prawa do ochrony danych osobowych, a także musi mieć charakter niezbędny i proporcjonalny.

Dla tych szczególnych celów rozporządzenie wymaga ze strony państw członkowskich wprowadzenia, lub zezwala im na wprowadzanie, przepisów uzupełniających. W przypadku badań historycznych i naukowych, a także przetwarzania danych dla celów statystycznych oraz archiwalnych, przepisy te mogą nawet stanowić podstawę prawną dla przetwarzania danych wrażliwych.

Inne szczególne zagadnienia, w których przewiduje się udział prawa państwa członkowskiego, obejmują przetwarzanie danych pracowników, przetwarzanie w związku z wolnością słowa i tajemnicą zawodową (w odniesieniu do którego przewidziane są ograniczenia uprawnień kontrolnych organów nadzorczych).

Administratorzy (a także, w niektórych przypadkach, podmioty przetwarzające dane) będą musieli przeanalizować i dostosować się do różnych strategii państw członkowskich w tych obszarach.

Co trzeba zrobić

- Należy ocenić czy przetwarzanie przez Państwa danych może podlegać wyjątkom lub warunkom szczególnym na mocy RODO.
- W przypadku, gdy dany wyjątek lub warunek szczególny może mieć zastosowanie do prowadzonego przez Państwa przetwarzania, należy zidentyfikować jurysdykcje, w których przetwarzanie ma miejsce.
- Należy także rozważyć możliwość wspierania dalszych prac legislacyjnych w państwach, na terytorium których mogą Państwo podlegać wprowadzonym w ten sposób lokalnym obostrzeniom.
- W przypadku, gdy zasady dotyczące tajemnicy zawodowej mają zastosowanie do danych osobowych otrzymywanych lub zbieranych przez administratora danych lub podmiot przetwarzający dane, należy zapewnić, że przedmiotowe dane są odpowiednio oznaczone w celu umożliwienia ich ochrony przed ujawnieniem organom nadzorczym.

Nieznane:

Wiele kategorii wyjątków i warunków szczególnych ma swoje odpowiedniki w postanowieniach dyrektywy w sprawie ochrony danych. Trudno jest jednak przewidywać zgodność ze wspomnianymi wyjątkami i warunkami szczególnymi ze względu na fakt, że zależą one od sposobu, w jaki państwa członkowskie wprowadzą lub utrzymają w mocy przepisy ustawowe i inne przepisy prawne w tym obszarze.

Komentarz

Przypadki szczególne

Przepisy RODO przewidują szerokie wyjątki i odstępstwa w dwóch najważniejszych obszarach: (1) w Rozdziale III Sekcji 5, w odniesieniu do *„ograniczeń”* obowiązków i praw w zakresie ochrony danych, oraz (2) w Rozdziale IX, w odniesieniu do *„szczególnych sytuacji związanych z przetwarzaniem”*.

Art. 23 - Ograniczenia

Art. 23 RODO przewiduje prawo państw członkowskich do wprowadzania wyjątków od zasad ochrony danych w pewnych sytuacjach; odpowiednie przepisy zawarte są także w dyrektywie w sprawie ochrony danych. Państwa członkowskie mogą wprowadzać wyjątki od obowiązków w zakresie przejrzystości i od praw osób, których dane dotyczą, jednak wyłącznie wtedy, gdy takie ograniczenie *„nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym”*.

Środki te mają za zadanie służyć:

- bezpieczeństwu narodowemu;
- obronie;
- bezpieczeństwu publicznemu;
- zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub naruszenia zasad etyki w zawodach regulowanych;
- innym ważnym interesom publicznym, w szczególności gospodarczym lub finansowym (np. kwestiom budżetowym i podatkowym);
- ochronie niezależności sądów i postępowania sądowego;
- sprawowaniu władzy publicznej w zakresie monitorowania, inspekcji i funkcji regulacyjnych związanych ze sprawowaniem władzy publicznej w zakresie bezpieczeństwa, obronności oraz w innym ważnym interesie publicznym lub w celu zapobiegania przestępczości;
- ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;
- dochodzeniu roszczeń cywilnoprawnych.

Aby środek był akceptowalny, musi (zgodnie z art. 23 ust. 2) zawierać szczególne postanowienia określające:

- cele lub kategorie przetwarzania;
- kategorie przetwarzanych danych;
- zakres ograniczeń, które w stosunku do przepisów RODO, wprowadza dany środek;
- zabezpieczenia zapobiegające nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu danych;
- administratorów, którzy mogą powoływać się na przedmiotowe ograniczenia;
- obowiązujące okresy przechowywania danych i środki zabezpieczające;
- ryzyko naruszenia praw lub wolności osoby, której dane dotyczą; oraz
- prawo osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

Art. 85-91: „szczególne sytuacje związane z przetwarzaniem”

Przepisy zawarte w Rozdziale IX RODO przewidują zestaw różnorodnych wyjątków i odstępstw oraz kompetencji do nakładania dodatkowych wymogów, w stosunku do praw i obowiązków wynikających z RODO, dla określonych rodzajów przetwarzania danych. Te różnorakie postanowienia stanowią rozwinięcie szczególnych sytuacji przetwarzania, które przewiduje dyrektywa w sprawie ochrony danych.

Art. 85: Wolność wypowiedzi i informacji

Ten przepis zobowiązuje państwa członkowskie do wprowadzenia odstępstw od przepisów RODO, koniecznych do „pogodzenia prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji”. Art. 85, pomimo że zakres jego zastosowania jest szerszy niż art. 9 dyrektywy w sprawie ochrony danych, reguluje w sposób szczególny przetwarzanie danych dokonywane dla celów dziennikarskich, a także akademickich, artystycznych lub literackich. Państwa członkowskie będą zobowiązane powiadomić Komisję o sposobie wykonania tego obowiązku oraz o każdej zmianie uchwalonych przepisów.

Art. 86: Publiczny dostęp do dokumentów urzędowych

Ten przepis stanowi rozwinięcie Motywu 72 dyrektywy w sprawie ochrony danych i pozwala na ujawnianie danych osobowych zawartych w dokumentach urzędowych zgodnie z przepisami prawa UE lub prawa danego państwa członkowskiego, zezwalającymi na publiczny dostęp do dokumentów urzędowych. Ujawnianie takich danych doznaje pewnych ograniczeń, gdyż przepisy te powinny, zgodnie z Motywem 154, *„godzić publiczny dostęp do dokumentów urzędowych (...) z prawem do ochrony danych osobowych”*. Dyrektywa 2003/98/EC w sprawie *„ponownego wykorzystywania informacji sektora publicznego”* nie zmienia zobowiązań po stronie organów publicznych ani też praw osób fizycznych wynikających z RODO.

Art. 87: Krajowe numery identyfikacyjne

Jest to powielenie, wynikającego z dyrektywy w sprawie ochrony danych, prawa państw członkowskich do ustalania własnych warunków przetwarzania krajowych numerów identyfikacyjnych. Jedynym rozwinięciem jest w tym przypadku wyjaśnienie, że wymaga to wdrożenia odpowiednich zabezpieczeń.

Art. 88: Dane pracowników

Państwa członkowskie mogą wprowadzać (w drodze ustaw lub porozumień zbiorowych) bardziej szczegółowe przepisy w zakresie przetwarzana danych osobowych pracowników, obejmujące wszystkie istotne aspekty zatrudnienia: od rekrutacji do rozwiązania stosunku pracy. Obejmuje to możliwość ustanowienia zasad określających to, kiedy w kontekście stosunku pracy zgoda na przetwarzanie danych jest ważną podstawą prawną. Wyżej wspomniane zasady muszą obejmować szczególne środki mające na celu zabezpieczenie "*godności, prawnie*

uzasadnionych interesów oraz podstawowych praw" osób, których dane dotyczą. Ponadto, RODO wspomina o przejrzystości przetwarzania danych, przekazywaniu danych wewnątrz grupy przedsiębiorstw i o systemach monitorowania jako obszarach, w których należy szczególnie wziąć pod uwagę te kwestie.

Państwa członkowskie są zobowiązane powiadamiać Komisję o wszelkich nowych przepisach wprowadzanych na mocy tego artykułu do czasu wejścia w życie RODO, a także o wszelkich zmianach w tychże przepisach.

Art. 89 ust. 1 i 2: Przetwarzanie dla celów badań naukowych i historycznych oraz dla celów statystycznych

Art. 89 ust. 1 potwierdza, że administratorzy mogą w tych celach przetwarzać dane, o ile wdrożą odpowiednie zabezpieczenia (więcej informacji na ten temat znajduje się w części poświęconej zgodności z prawem przetwarzania i dalszego przetwarzania danych, a także danym wrażliwym i przetwarzaniu zgodnie z prawem). O ile to możliwe, administratorzy danych powinni w tych celach przetwarzać dane, które nie pozwalają, lub już nie pozwalają, na identyfikację osób, których dane dotyczą. W przypadku, gdy anonimizacja danych nie jest możliwa, należy zastosować technikę pseudonimizacji, chyba że także ten środek mógłby negatywnie wpływać na cel prowadzenia badań naukowych i statystycznych.

Art. 89 ust. 2 zezwala państwom członkowskim i Unii na ustanowienie w ich porządkach prawnych wyjątków od praw osób, których dane dotyczą w zakresie dostępu, sprostowania, ograniczenia przetwarzania i wyrażania sprzeciwu (z zastrzeżeniem zabezpieczeń określonych w art. 89 ust. 1), jeśli wspomniane prawa „*uniemożliwiają lub poważnie utrudniają*" osiągnięcie określonych celów, a wprowadzenie wyjątków jest konieczne do sprostania przedmiotowym wymogom.

Preambuła doprecyzowuje sposób, w jaki „*badania naukowe*", „*badania historyczne*" oraz „*cele statystyczne*" powinny być interpretowane. Motyw 159 stwierdza, że badania naukowe należy „*interpretować szeroko*", tak by obejmowały badania finansowane ze źródeł prywatnych, a także studia prowadzone w interesie publicznym. Aby móc uznać przetwarzanie danych za mające charakter statystyczny, zgodnie z Motywem 162, wynik takiego przetwarzania nie powinien mieć charakteru „danych osobowych, lecz danych zbiorczych" i nie powinien stanowić podstawy środków lub decyzji dotyczących konkretnych osób fizycznych.

Art. 89 ust. 1 i 3: Przetwarzanie do celów archiwalnych w interesie publicznym

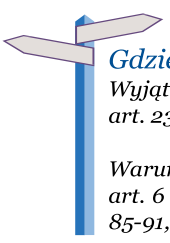
Do „*przetwarzania do celów archiwalnych w interesie publicznym*", stosują się te same wyjątki i zabezpieczenia co do przetwarzania dla celów badań naukowych oraz celów statystycznych, z tym że wyjątki te mogą zostać ustanowione w zakresie prawa do przenoszenia danych. Motyw 158 zawiera dodatkowe informacje na ten temat sugerując, że na ten przepis powinny powoływać się jedynie organy lub władze, na które prawo Unii bądź danego państwa członkowskiego nakłada obowiązek dokonywana operacji na wpisach o „*trwałej wartości dla ogólnego interesu publicznego*".

Artykuł 90: Obowiązek zachowania tajemnicy

Ten przepis zezwala państwom członkowskim na wprowadzenie przepisów szczególnych mających na celu ochronę „*tajemnicy zawodowej*" lub „*innej równoważnej tajemnicy*" wobec organów nadzorczych, uprawnionych do dostępu do danych osobowych lub zajmowanych pomieszczeń. Zasady te muszą „*godzić prawo do ochrony danych osobowych z obowiązkiem zachowania tajemnicy*", i mogą mieć zastosowanie wyłącznie do danych zebranych bądź otrzymanych z zastrzeżeniem obowiązku zachowania tej tajemnicy. Także w tym przypadku państwa członkowskie są zobowiązane powiadamiać Komisję o wszelkich nowych przepisach wprowadzonych na mocy tego artykułu do czasu wejścia w życie RODO, a także o wszelkich zmianach tychże przepisów.

Artykuł 91: Kościoły i związki wyznaniowe

Ten przepis chroni obowiązujące dotychczas „*szczegółowe*" zasady stosowane przez kościoły, związki i wspólnoty wyznaniowe, pod warunkiem że zasady te zostaną dostosowane do RODO. Takie podmioty nadal będą podlegać kontroli niezależnego organu nadzorczego na mocy przepisów Rozdziału VI (więcej informacji znajduje się w części poświęconej współpracy i spójności pomiędzy organami nadzorczymi).



Gdzie mogę to znaleźć?
Wyjątki
art. 23, motyw 73

Warunki szczególne
art. 6 ust. 2 i 3, art. 9 ust. 2 lit. a), art. 85-91, motywy 50, 53, 153-165

Akty delegowane, akty wykonawcze i przepisy końcowe

Na pierwszy rzut oka

Końcowe rozdziały RODO stanowią, że rozporządzenie ma zastosowanie od 25 maja 2018 r. Określają również stosunek RODO do innych aktów prawnych Unii dotyczących ochrony danych, w tym dyrektywy o prywatności i łączności elektronicznej.

Po wejściu w życie RODO Komisja będzie regularnie przedkładać sprawozdania dotyczące tego rozporządzenia. Ponadto przepisy końcowe upoważniają Komisję do przyjmowania pewnych aktów delegowanych uzupełniających RODO (np. w odniesieniu do stosowania standardowych znaków graficznych i mechanizmów certyfikacji).

Co trzeba zrobić

- Należy pamiętać, że RODO ma zastosowanie od 25 maja 2018 r.
- W związku z tym należy zawczasu zaplanować zmiany, jakie trzeba będzie wprowadzić w celu sprostania nowym wymaganiom. Więcej informacji znajduje się w podsumowaniach poprzednich części.
- Jeśli dotyczy to Państwa przedsiębiorstwa, należy obserwować rozwój wydarzeń w związku z dyrektywą o prywatności i łączności elektronicznej. 10 stycznia 2017 r. Komisja Europejska przyjęła projekt rozporządzenia w sprawie prywatności i łączności elektronicznej, mającego zastąpić dyrektywę o prywatności i łączności elektronicznej.

Stopień zmian

Komentarz

Rozdział 10 RODO upoważnia Komisję do przyjmowania aktów delegowanych (w odniesieniu do standardowych znaków graficznych, zgodnie z art. 12 ust. 8, oraz w odniesieniu do mechanizmów certyfikacji, zgodnie z art. 43 ust. 8. Upoważnienia mogą zostać cofnięte przez Parlament lub Radę w każdym czasie. Przyjęte akty wejdą w życie z upływem 3 miesięcy, o ile w tym czasie ani Parlament, ani Rada, nie wyrażą sprzeciwu. Powyższy termin może zostać wydłużony. Komisję będzie w tych pracach wspierał komitet powołany zgodnie z Rozporządzeniem nr 182/2011. Szczególnie ważne jest, aby Komisja w ramach prac przygotowawczych przeprowadziła odpowiednie konsultacje, w tym na szczeblu eksperckim (motyw 166).

Komisji powierzono także uprawnienia wykonawcze w celu zapewnienia jednolitych warunków wdrażania przepisów RODO. Uprawnienia te powinny być wykonywane zgodnie z Rozporządzeniem nr 182/2011.

Rozdział 11 RODO stanowi, że dyrektywa w sprawie ochrony danych zostanie uchylona po wejściu w życie RODO, tj. z upływem dwóch lat i dwudziestu dni od jego publikacji w Dzienniku Urzędowym (25 maja 2018 r.). Odesłania do uchylonej dyrektywy w sprawie ochrony danych, zawarte w innych aktach prawnych, należy traktować jako odesłania do RODO.

Komisja będzie regularnie przedkładać Parlamentowi i Radzie sprawozdania dotyczące RODO, ze szczególnym uwzględnieniem przepisów o przekazywaniu danych oraz o współpracy i spójności. Pierwsze sprawozdanie powinno zostać przedłożone nie później niż 4 lata od wejścia w życie RODO, a kolejne – co 4 lata od tej daty. Sprawozdania te będą podawane do wiadomości publicznej.

Art. 95 wyjaśnia, że RODO nie nakłada dodatkowych obowiązków na dostawców publicznie dostępnych usług łączności elektronicznej w ramach Unii, w zakresie w jakim podlegają oni szczegółowym obowiązkom mającym ten sam cel, określonym w dyrektywie o prywatności i łączności elektronicznej. 10 stycznia 2017 r. Komisja Europejska przyjęła projekt rozporządzenia w sprawie prywatności i łączności elektronicznej, mającego zastąpić dyrektywę o prywatności i łączności elektronicznej.

Motyw 171 stanowi, że w przypadku, gdy przetwarzanie jest oparte na zgodzie udzielonej w myśl obowiązującej dyrektywy w sprawie ochrony danych, osoba, której dane dotyczą, nie musi ponownie wyrażać zgody, jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom RODO.

Gdzie mogę to znaleźć?
art. 92-99, motywy 166-173

Słowniczek

Grupa Robocza Art. 29
W skład Grupy Roboczej Art. 29 („Grupy Roboczej") wchodzą przedstawiciele organów nadzorczych Państw członkowskich, Europejskiego Inspektora Ochrony Danych („EIOD") oraz Komisji Europejskiej. Grupa Robocza została przekształcona w Europejską Radę Ochrony Danych o podobnym składzie, jednakże z niezależnym sekretariatem (więcej informacji znajduje się w części poświęconej Europejskiej Radzie Ochrony Danych).

Administrator danych osobowych
Osoba lub organ, który samodzielnie lub wraz z innymi osobami lub organami określa cele i środki przetwarzania danych osobowych.

Podmiot przetwarzający
Podmiot, który przetwarza dane osobowe w imieniu administratora danych.

Dyrektywa w sprawie ochrony danych
Dyrektywa nr 95/46/WE, która regulowała dotąd kwestie przetwarzania danych osobowych na terytorium Unii Europejskiej i która zostanie zastąpiona przez RODO.

Inspektor ochrony danych
Inspektor ochrony danych, którego wyznaczenie jest obowiązkowe, gdy (i) przetwarzania dokonuje podmiot publiczny lub gdy (ii) „główna działalność" administratora danych lub podmiotu przetwarzającego wymaga (a) „regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę" lub (b) polega na przetwarzaniu "na dużą skalę" szczególnych kategorii danych lub danych dotyczących wyroków skazujących.

EROD
Europejska Rada Ochrony Danych ("EROD") zastąpi Grupę Roboczą. Jej zadania będą obejmować zapewnianie spójności stosowania przepisów RODO, doradzanie Komisji Europejskiej, wydawanie wytycznych, kodeksów dobrych praktyk i zaleceń, akredytowanie podmiotów certyfikujących oraz wydawanie opinii na temat projektów decyzji organów nadzorczych.

EOG
Europejski Obszar Gospodarczy obejmuje 28 państw członkowskich UE oraz Islandię, Liechtenstein i Norwegię. Nie obejmuje natomiast Szwajcarii.

RODO
Rozporządzenie ogólne o ochronie danych osobowych uchwalone ostatecznie 27 kwietnia 2016 r. jako Rozporządzenie (UE) 2016/679. Niniejsze wydanie Przewodnika uwzględnia wytyczne opublikowane przez Grupę Roboczą w grudniu 2016 r.

Dane osobowe
Wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej zwanej „osobą, której dane dotyczą". Osoba, której dane dotyczą to osoba fizyczna, którą można bezpośrednio lub pośrednio zidentyfikować.

Ocena skutków dla ochrony danych
RODO nakłada na administratora danych i podmioty przetwarzające dane nowy obowiązek przeprowadzenia oceny skutków dla ochrony danych (zwanej również oceną skutków dla prywatności) przed podjęciem operacji przetwarzania danych, która – ze względu na swój charakter, zakres lub cele – może nieść za sobą wysokie ryzyko dla prywatności. Rozdział IV Sekcja 3 zawiera niewyczerpujące wyliczenie kategorii przetwarzania danych, objętych zakresem zastosowania tego przepisu.

Przetwarzanie
Przetwarzanie zostało zdefiniowane szeroko, jako jakakolwiek operacja lub zespół operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. Przykładami przetwarzania jest zbieranie, utrwalanie, organizowanie, przechowywanie, wykorzystywanie i niszczenie danych osobowych.

Pseudonimizacja
Technika polegająca na przetwarzaniu danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i zostały poddane zabezpieczeniom technicznymi i organizacyjnymi uniemożliwiającymi ich ponowne przypisanie tej osobie.

Prawo do usunięcia danych / prawo do bycia zapominanym
Dotychczasowe prawo do usunięcia danych osobowych, przyznane osobie, której dane dotyczą, zostało rozszerzone zgodnie z przepisami Rozdziału III Sekcji 3 RODO

Szczególne kategorie danych
Znane również jako "dane wrażliwe". RODO rozszerzyło definicję szczególnych kategorii danych, tak by obejmowała zarówno dane biometryczne, jak i genetyczne.

Prawo dostępu
Jest to uprawnienie osoby, której dane dotyczą, do żądania od administratora udzielenia określonych informacji dotyczących przetwarzania jej danych osobowych zgodnie z przepisami Rozdziału III Sekcji 2 RODO.

Organ nadzorczy/organ wiodący
Organy nadzorcze to krajowe organy właściwe w sprawach ochrony danych, do których kompetencji należy zapewnienie przestrzegania RODO w danym państwie członkowskim.

Pojęcie "one-stop-shop" – jeśli przedsiębiorca ma jednostki organizacyjne w więcej niż jednym państwie członkowskim, "organ wiodący" wyznacza się ze względu na położenie jego głównej jednostki organizacyjnej w Unii. Pewne funkcje regulacyjne może wykonywać także organ nadzorczy niebędący organem wiodącym, np. w przypadku gdy przetwarzanie oddziałuje na sytuację osób, których dane dotyczą, w państwie, w którym działa ten organ.

Przekazanie
Przekazanie danych osobowych do państw spoza EOG lub do organizacji międzynarodowych, poddane obostrzeniom przewidzianym w Rozdziale V RODO. Podobnie jak pod rządami dyrektywy w sprawie ochrony danych, przekazanie danych nie wymaga ich fizycznego przemieszczenia. Przekazaniem danych, dla celów RODO, jest już samo uzyskanie wglądu do danych przechowywanych w innej lokalizacji.

Przedsiębiorca
Pojęcie to pojawia się w RODO w rozmaitych kontekstach, najczęściej w odniesieniu do podmiotu prawnego prowadzącego „działalność gospodarczą". Pojęcie to ma szczególne znaczenie w kontekście przepisów RODO o karach finansowych. Przedsiębiorca podlega karom finansowym, obliczonym jako procent osiągniętego przezeń całkowitego rocznego światowego obrotu za poprzedni rok obrotowy. W tym kontekście pojęcie przedsiębiorcy nawiązuje do dorobku unijnego prawa ochrony konkurencji.

Kontakt

Piotr Dynowski LL.M.

Partner

+48 22 583 79 14

piotr.dynowski@twobirds.com

Izabela Kowalczuk-Pakuła

Counsel

+48 22 583 79 32

izabela.kowalczuk-pakula@twobirds.com

twobirds.com

Aarhus & Abu Dhabi & Bratysława & Bruksela & Budapeszt & Dubaj & Düsseldorf & Frankfurt & Haga & Hamburg & Helsinki & Hong Kong & Kopenhaga & Londyn & Luksemburg & Lyon & Madryt & Mediolan & Monachium & Paryż & Pekin & Praga & Rzym & Singapur & Sydney & Szanghaj & Sztokholm & Warszawa