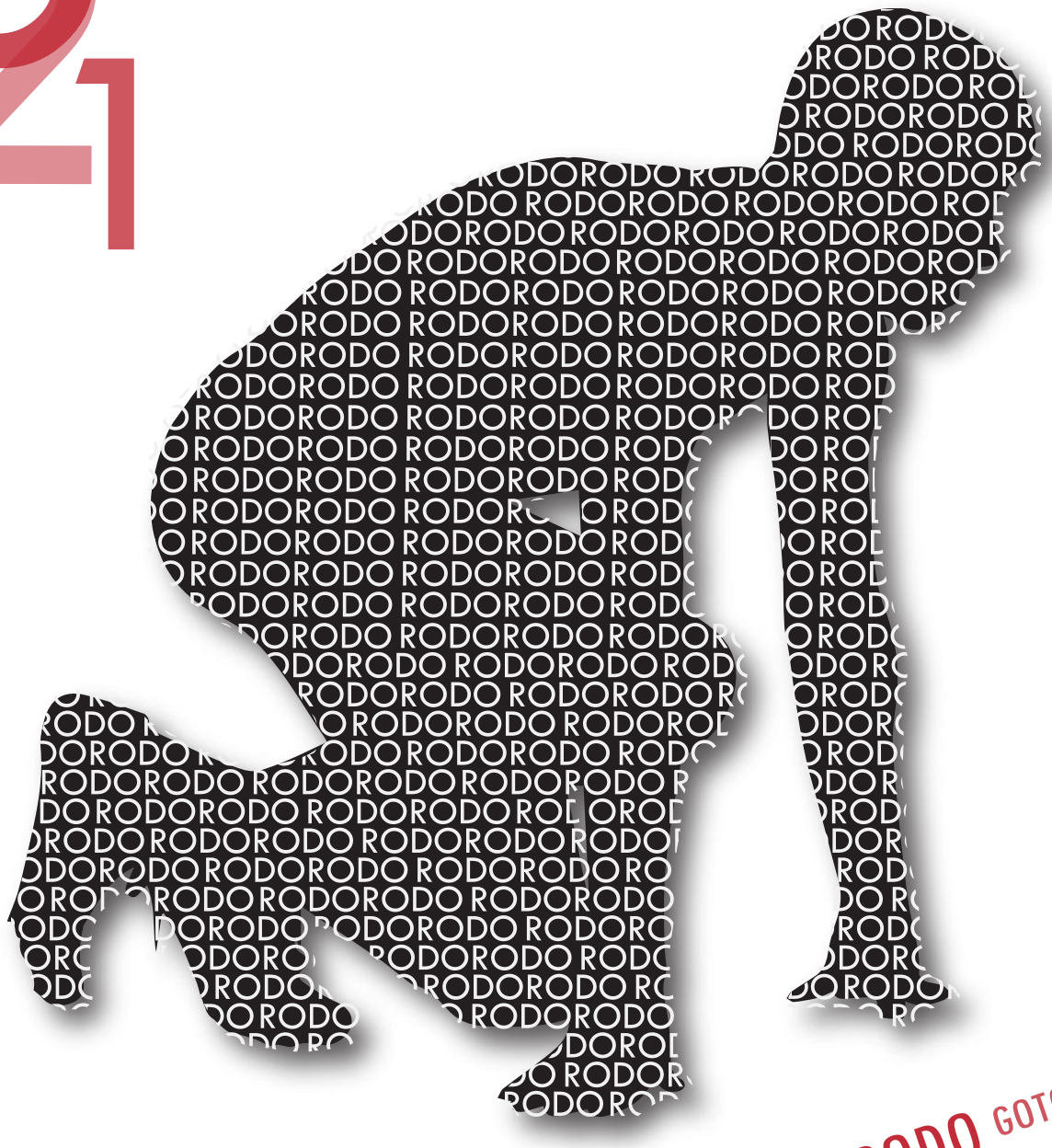
Narodowy Instytut Wolności
Centrum Rozwoju Społeczeństwa Obywatelskiego

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

2018



GOTOWI NA RODO GOTOWI NA RODO GOTOWI NA RODO GOTOWI NA RODO GOTOWI NA RODO

GOTOWI NA RODO

PRZYDATNE DEFINICJE

Administrator
osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Osoba, której dane dotyczą
osoba fizyczna, możliwa do zidentyfikowania na podstawie określonych danych osobowych;

Dane osobowe
informacje o osobie fizycznej takie jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczegółów określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Szczególna kategoria danych osobowych
dane wrażliwe, czyli dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne lub dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej.

Zgoda
dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba fizyczna, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

Przetwarzanie
oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych, w sposób zautomatyzowany lub niezautomatyzowany, np.: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Podmiot przetwarzający
osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

Anonimizacja
proces uniemożliwiający zidentyfikowanie osoby fizycznej na podstawie określonych danych

Pseudonimizacja
przetworzenie 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 są objęte technicznymi i organizacyjnymi środkami bezpieczeństwa, które uniemożliwiają ich wykorzystanie w celu zidentyfikowania osoby fizycznej;

Profilowanie
dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny osoby fizycznej, w szczególności do analizy lub prognozy efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania;

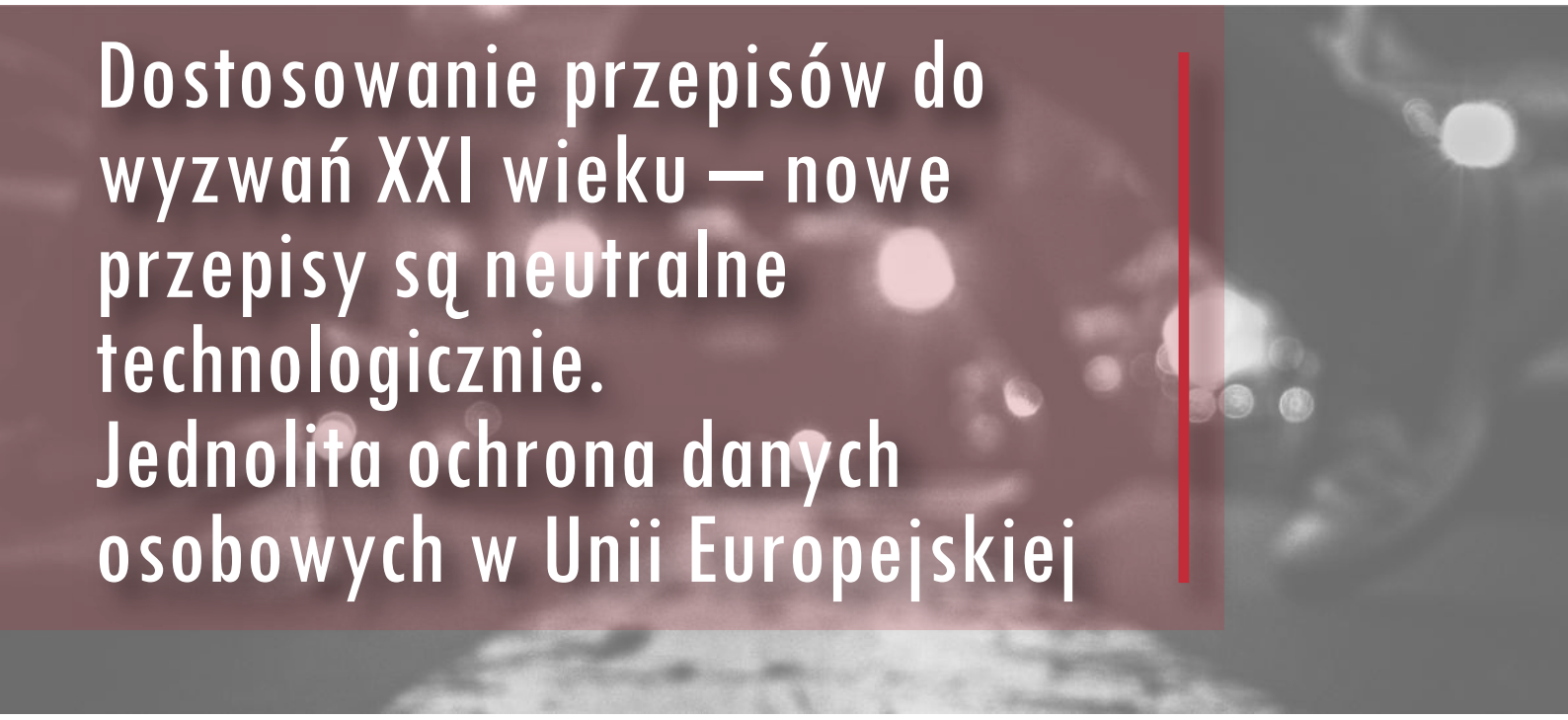
Główna jednostka organizacyjna
w przypadku administratora posiadającego jednostki w kilku państwach UE będzie to miejsce siedziby jednostki organizacyjnej, w której zapadają decyzje dotyczące przetwarzania danych osobowych, albo miejsce siedziby centralnej administracji.

1.1. CO OZNACZA RODO

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

RODO ma na celu wzmocnienie podstawowych praw obywateli w epoce cyfrowej i ułatwienie przedsiębiorstwom i organizacjom działania na wspólnym rynku. RODO ma zastosowanie od 25 maja 2018 r.

Nowe unijne przepisy o ochronie danych osobowych wpływają na krajowe przepisy w tym zakresie. Z uwagi na to prowadzone są prace nad nową ustawą o ochronie danych osobowych, która ma zapewnić skuteczne stosowanie przepisów rozporządzenia.



1.2. NOWE PRZEPISY - NOWE KORZYŚCI

Dotychczasowe przepisy dotyczące ochrony danych osobowych obowiązywały w Unii Europejskiej od 1995 r., jednak kwestia ochrony danych dotychczas nie stanowiła ważnego obszaru zarządzania przedsiębiorstwem czy organizacją. Wynikało to m.in. z braku realnych kar administracyjnych za nieprzestrzeganie przepisów.

Rozwój Internetu spowodował wzrost zainteresowania ochroną danych w społeczeństwie. Dzisiaj dane są walutą gospodarki cyfrowej. Zbierane, analizowane i przekazywane na całym świecie zyskały ogromne znaczenie gospodarcze.

Zbierane, analizowane i przekazywane na całym świecie zyskały ogromne znaczenie gospodarcze.

Według szacunków wartość danych osobowych obywateli państw europejskich może sięgnąć 1 biliona euro do 2020 r. Nowe przepisy wspierają rozwój gospodarczy i rozwój wspólnego rynku cyfrowego: z jednej strony wzmacniają ochronę praw indywidualnych osób, a z drugiej – wprowadzają ułatwienia dla przedsiębiorców.

Najważniejsze korzyści z wdrożenia RODO

„Prawo do bycia zapomnianym" pomoże w lepszym zarządzaniu ryzykiem dotyczącym ochrony danych online. Jeżeli dana osoba nie chce, aby nadal przetwarzano jej dane i jeżeli nie istnieją żadne uzasadnione powody ich przechowywania, dane zostaną usunięte.

Prawo nieodpłatnego i łatwego dostępu do własnych danych osobowych - dzięki temu dana osoba łatwiej może sprawdzić jakie informacje na jej temat znajdują się w posiadaniu przedsiębiorstw i organów publicznych, oraz przenosić dane osobowe między usługodawcami (prawo do przenoszenia danych).

DLA OSÓB INDYWIDUALNYCH

Obowiązek informowania o naruszeniu danych osobowych - jeżeli dojdzie do naruszenia danych, przedsiębiorstwa i organizacje będą musiały niezwłocznie o nich powiadomić organ nadzorczy oraz osoby, których dane dotyczą.

Przejrzystość przetwarzania danych osobowych – informacje o przetwarzaniu mają być łatwo zrozumiałe, w szczególności kiedy są kierowane do dzieci.

Łatwiejsze egzekwowanie prawa do ochrony danych osobowych - prawo do ochrony danych ma być skutecznie egzekwowane dzięki ulepszeniu procedur administracyjnych i sądowych w przypadkach naruszenia.

Najważniejsze korzyści z wdrożenia RODO DLA MAŁYCH I ŚREDNICH ORGANIZACJI

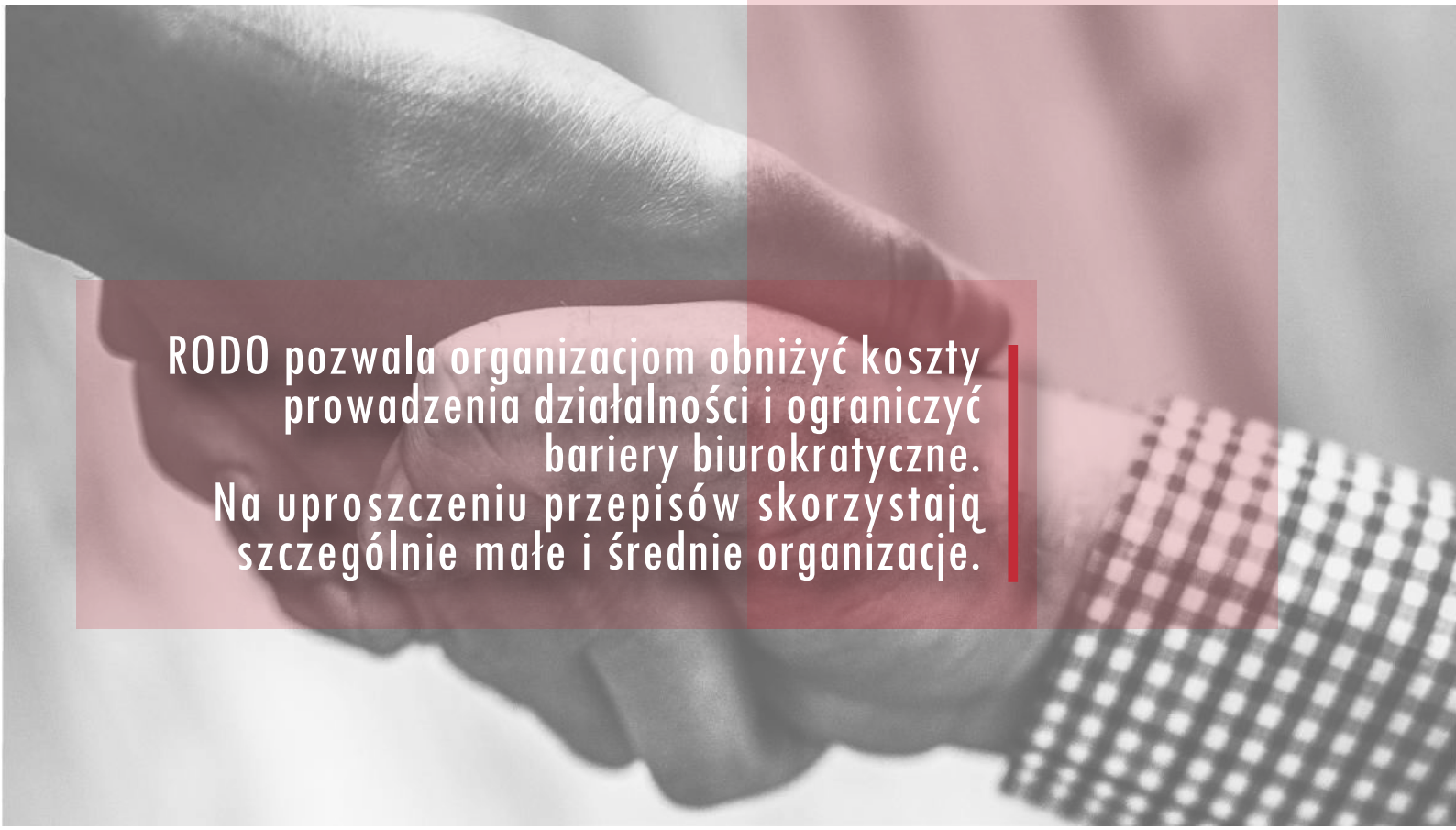
Brak obowiązku wyznaczenia Inspektora Ochrony Danych (IOD-a) – taka konieczność będzie dotyczyć tylko organizacji, dla których przetwarzanie danych jest główną działalnością – z racji swego charakteru, zakresu lub celów – np. w przypadku pozyskiwania talentów, profilowania osób fizycznych. W małych organizacjach nie ma wymogu zatrudniania takiej osoby w pełnym wymiarze czasu. Może to być konsultant udzielający porad doraźnie, co znacznie ogranicza koszty.

Jeśli chodzi o wymóg dokonywania tzw. oceny skutków w zakresie ochrony danych, jej kryteria bardzo zawężone – obejmują tylko bardzo ryzykowne działania związane z przetwarzaniem danych (np. zakrojone na dużą skalę systemy obejmujące zbiory danych genetycznych lub danych biometrycznych).

Brak obowiązku sporządzania dokumentacji dotyczącej działań związanych z przetwarzaniem danych, chyba że przetwarzanie to odbywa się systematycznie lub wiąże się z ryzykiem dla praw i wolności osób, których dane dotyczą.

Brak obowiązku informowania o naruszeniu danych, chyba że naruszenie to wiąże się z wysokim ryzykiem dla praw i wolności osób, których dane dotyczą.

Brak obowiązku powiadamiania organów ochrony danych o danych osobowych przetwarzanych przez organizacje.



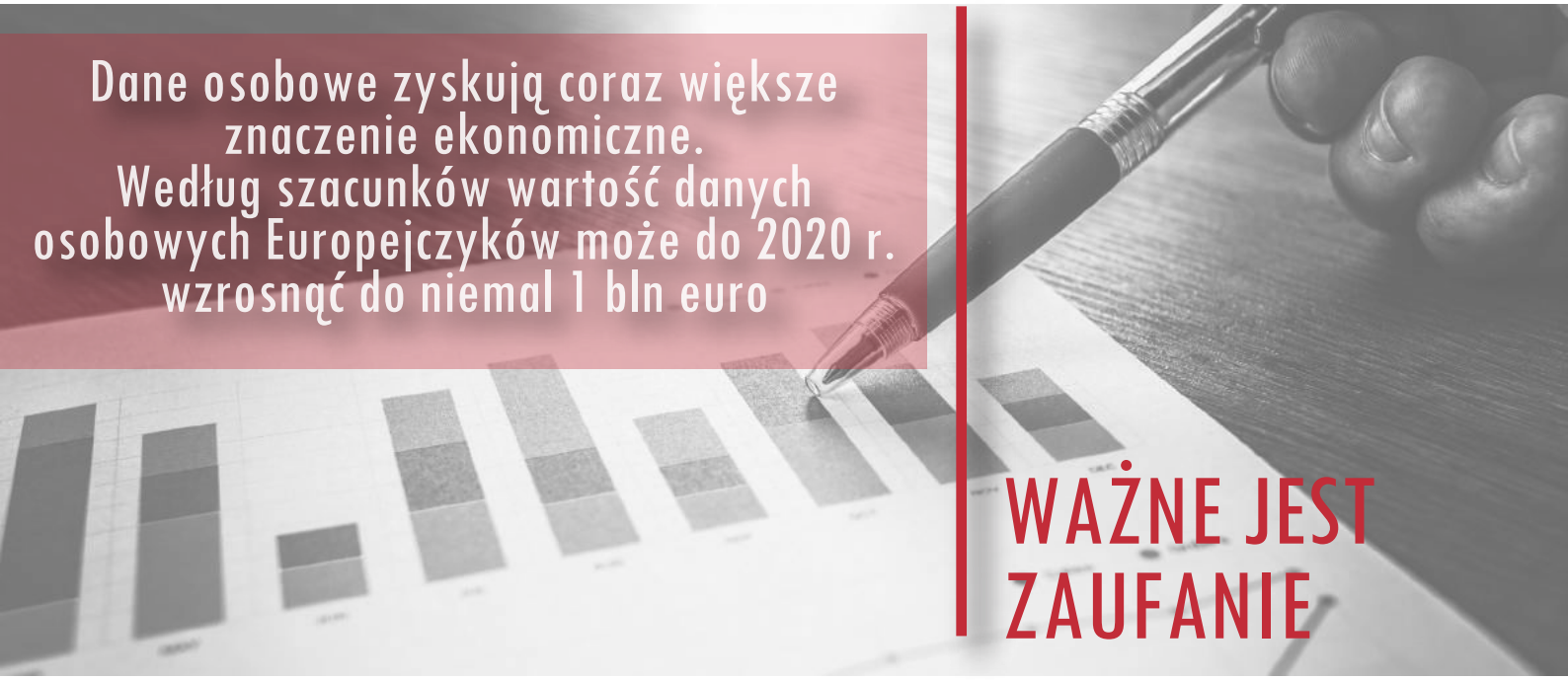
RODO pozwala organizacjom obniżyć koszty prowadzenia działalności i ograniczyć bariery biurokratyczne. Na uproszczeniu przepisów skorzystają szczególnie małe i średnie organizacje.

1.3. BUDOWANIE WIZERUNKU ORGANIZACJI A OCHRONA DANYCH OSOBOWYCH

Reforma ochrony danych pomoże przedsiębiorstwom i organizacjom zbudować zaufanie społeczeństwa do oferowanych przez nie usług. Według wyników badania Eurobarometr z 2015 r. , osiem na dziesięć osób ma poczucie, że nie ma pełnej kontroli nad swoimi danymi osobowymi. Dwie trzecie społeczeństwa czuje, że nie ma pełnej kontroli nad swoimi danymi w internecie. Przedsiębiorstwa i organizacje, które nie chronią należycie danych osobowych swoich klientów ryzykują, że stracą ich zaufanie.

Szczególnie w środowisku online to zaufanie jest niezbędne, aby zachęcać klientów do korzystania z nowych produktów i usług.

Dla przedsiębiorców i organizacji dane osobowe mogą mieć duże znaczenie finansowe, a klienci i inne osoby, których dane dotyczą, coraz świadomiej podchodzą do kwestii ochrony swoich danych. Organizacja przetwarzająca dane zgodnie z RODO to organizacja odpowiedzialna, która szanuje prawa klientów.



Dane osobowe zyskują coraz większe znaczenie ekonomiczne. Według szacunków wartość danych osobowych Europejczyków może do 2020 r. wzrosnąć do niemal 1 bln euro

WAŻNE JEST ZAUFANIE

Ponad 75% Europejczyków przyznało się do braku zaufania do firm internetowych, takich jak dostawcy wyszukiwarek, portali społecznościowych itp.

1/2 europejskich internautów obawia się, że stanie się ofiarą oszustwa polegającego na niewłaściwym wykorzystaniu ich danych

Tylko 28% osób stwierdziło, że zdaje sobie sprawę, która firma przetwarza ich dane prawidłowo

Mniej niż 33% Europejczyków ufa operatorom sieci telefonicznych i dostawcom internetu

89% Europejczyków opowiedziało się za równymi prawami do ochrony w całej UE

80% badanych stwierdziło, że są bardziej skłonni nabywać produkty i usługi firm, które zapewniają właściwą ochronę danych

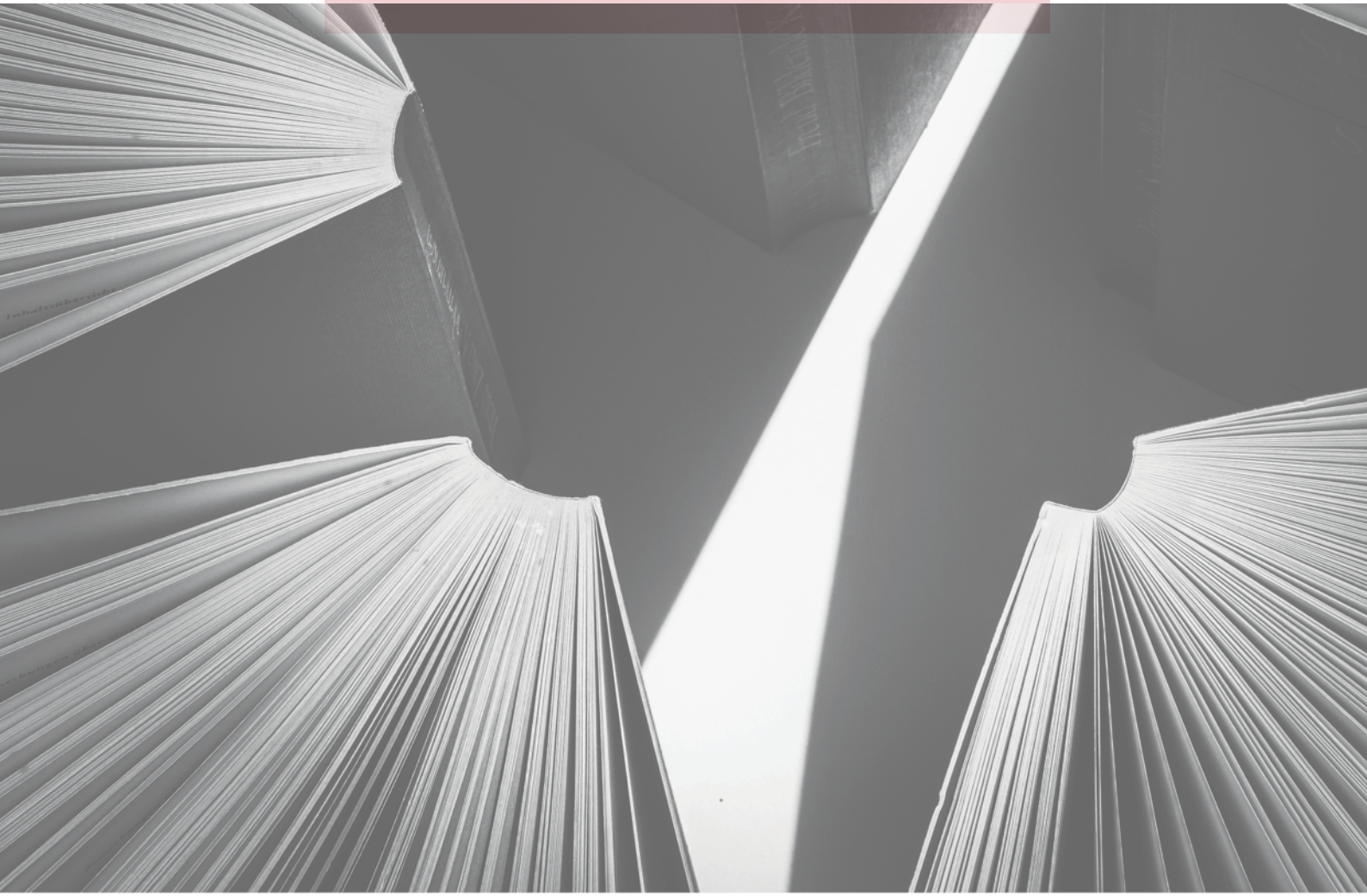
Na podstawie:
Eurobarometr, badanie specjalne 431 – „Data protection" („Ochrona danych"), wydanie z czerwca 2015 r.
Deloitte University Press, Building consumer trust, Protecting personal data in the consumer product industry; Consumer responses from the consumer product consumer and executive survey on data privacy and security.

2. KOGO DOTYCZĄ NOWE PRZEPISY

RODO obowiązuje organizacje, które przetwarzają dane osobowe w związku z działalnością prowadzoną w Unii Europejskiej, niezależnie od tego, czy samo przetwarzanie danych odbywa się w Unii.
Rozporządzenie obowiązuje również określone grupy podmiotów spoza UE, które nie mają jednostek organizacyjnych w Unii, ale ich czynności przetwarzania wiążą się z:

oferowaniem towarów lub usług osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty;

monitorowaniem zachowania osób fizycznych, o ile do zachowania tego dochodzi w Unii.



RODO ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną w Unii Europejskiej przez przedsiębiorstwo lub organizację – czyli administratora danych lub podmiot przetwarzający, niezależnie od tego, czy samo przetwarzanie danych odbywa się w Unii.

3.1. DANE OSOBOWE - CO TO ZNACZY?

Dane osobowe oznaczają każdą informację, która umożliwia zidentyfikowanie osoby. Możemy do nich zaliczyć:

- IMIĘ I NAZWISKO
- NUMER TELEFONU
- DOKUMENTACJĘ ZDROWOTNĄ
- NR IP KOMPUTERA
- IMIENNY ADRES E-MAILOWY
- PRZYCHÓD I DANE BANKOWE
- ADRES DOMOWY

Dane poddane pseudonimizacji* również podlegają wymogom RODO, ale już dane zanonimizowane** w taki sposób, że nie ma możliwości połączenia ich z konkretną osobą, są wyłączone z zakresu rozporządzenia.

RODO jest neutralne technologicznie, co oznacza, że dane osobowe są objęte ochroną bez względu na to, w jaki sposób są używane lub przechowywane – czy wykorzystujemy najnowszy system informatyczny, czy papierowe dokumenty w segregatorach, w każdym z tych przypadków przetwarzanie danych podlega wymogom RODO.

*,**
Zobacz: Przydatne definicje

PRZETWARZANIE TO:

ZBIERANIE

UTRWALANIE

ORGANIZOWANIE

PORZĄDKOWANIE

PRZECHOWYWANIE

DOSTOSOWYWANIE LUB ZMIENIANIE

POBIERANIE

PRZEGLĄDANIE

WYKORZYSTYWANIE

UJAWNIANIE POPRZEZ PRZESŁANIE

ROZPOWSZECHNIANIE LUB INNEGO

RODZAJU UDOSTĘPNIANIE

DOPASOWYWANIE LUB ŁĄCZENIE

OGRANICZANIE

USUWANIE LUB NISZCZENIE

Pamiętaj!

Zbieranie danych osobowych to również przetwarzanie.

3.3. NOWE PODEJŚCIE DO OCHRONY DANYCH OSOBOWYCH

Podejście oparte na ryzyku

RODO nie zmienia istotnie podstaw prawnych czy zasad przetwarzania danych osobowych. Wprowadza jednak nowe przepisy, które zwiększają samodzielność, ale i odpowiedzialność administratorów danych.

W praktyce oznacza to np., że obecne przepisy wymagające zawiadamiania GIODO o przetwarzaniu danych osobowych (obowiązek zgłaszania zbiorów do rejestracji) przestają obowiązywać. W ich miejsce RODO wprowadza skuteczne procedury dotyczące tych operacji przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Podejście oparte na ryzyku określa sposób, w jaki należy podchodzić do przetwarzania danych – w każdej sytuacji, kiedy zbieramy i korzystamy z danych osobowych, musimy przede wszystkim analizować ryzyko, jakie to przetwarzanie może spowodować dla prywatności osób, których te dane dotyczą.

Zasada rozliczalności

Zupełnie nową zasadą wprowadzoną przez rozporządzenie jest zasada rozliczalności. Zgodnie z nią, żeby spełnić wymogi rozporządzenia, każdy administrator danych ma obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych.

Rozporządzenie nie podaje jednak konkretnych przykładów najlepszych rozwiązań. Nie określa też minimalnych standardów technicznych zabezpieczenia danych (zachęca jedynie do skorzystania z narzędzi pseudonimizacji czy też szyfrowania danych).

Co istotne, przestaje też obowiązywać rozporządzenie MSWiA określające warunki techniczne i organizacyjne, jakie muszą spełniać urządzenia i systemy informatyczne wykorzystywane do przetwarzania danych osobowych.

Od 25 maja 2018 r. każdy administrator - biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych - musi samodzielnie zdecydować, jakie zabezpieczenia, dokumentację i procedury przetwarzania danych wdrożyć.

Pomocne w podjęciu tych decyzji mogą być wskazane w RODO dokumenty, takie jak zatwierdzane przez GIODO tzw. kodeksy postępowania, a także mechanizm certyfikacji, wytyczne Europejskiej Rady Ochrony Danych lub sugestie inspektora ochrony danych. Ponadto źródłem praktycznej i sprawdzonej wiedzy w zakresie budowy i zarządzania środkami bezpieczeństwa mogą być również np. normy ISO.

Z zasady rozliczalności wynika, że administrator ma obowiązek wykazania przestrzegania prawa. Oznacza to konieczność sporządzenia dokumentacji z wdrożenia instrumentów takich, jak:

- ocena skutków dla ochrony danych;
- wdrożenie zasady uwzględniania ochrony danych w fazie projektowania i zasady domyślnej ochrony danych (patrz dalej);
- stosowanie zatwierdzonych kodeksów postępowania.

3.3. NOWE PODEJŚCIE DO OCHRONY DANYCH OSOBOWYCH

Zasada uwzględniania ochrony danych w fazie projektowania i zasada domyślnej ochrony danych. Ochrona prywatności powinna być brana pod uwagę i stosowana w praktyce przy prowadzeniu wszelkich projektów i działań, tak w sferze publicznej, jak i prywatnej. Oznacza to prawnie wiążący obowiązek uwzględnienia ochrony danych w fazie projektowania oraz zasadę domyślnej ochrony danych.

Uwzględnianie ochrony danych w fazie projektowania zakłada, że ochrona prywatności powinna być wbudowana w każdy nowy projekt. Oznacza to, że prywatność będzie chroniona nie poprzez dodatki do systemu lub nakładki przygotowane na już istniejące rozwiązania, lecz jest wbudowana w jego konstrukcję od początku, jako składowa projektu.

Zasada domyślnej ochrony danych oznacza konieczność zapewnienia jak najdalej posuniętych zabezpieczeń prywatności w ustawieniach początkowych każdego systemu czy platformy internetowej. Zabezpieczenia mają być ustawione domyślnie, czyli bez konieczności jakiegokolwiek działania osób, których dane dotyczą – i to w kluczowym dla użytkownika momencie przyłączenia się do danego systemu lub wejścia na stronę internetową. Co więcej, domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu, dla którego zostały zebrane (minimalizacja danych).

Zasady te tworzą solidne ramy ochrony praw i wolności osób, których dotyczą.

Przetwarzanie danych osobowych w świetle RODO podlega również następującym zasadom:

zgodności z prawem, rzetelności i przejrzystości – przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;

ograniczonego przechowywania – dane mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami);

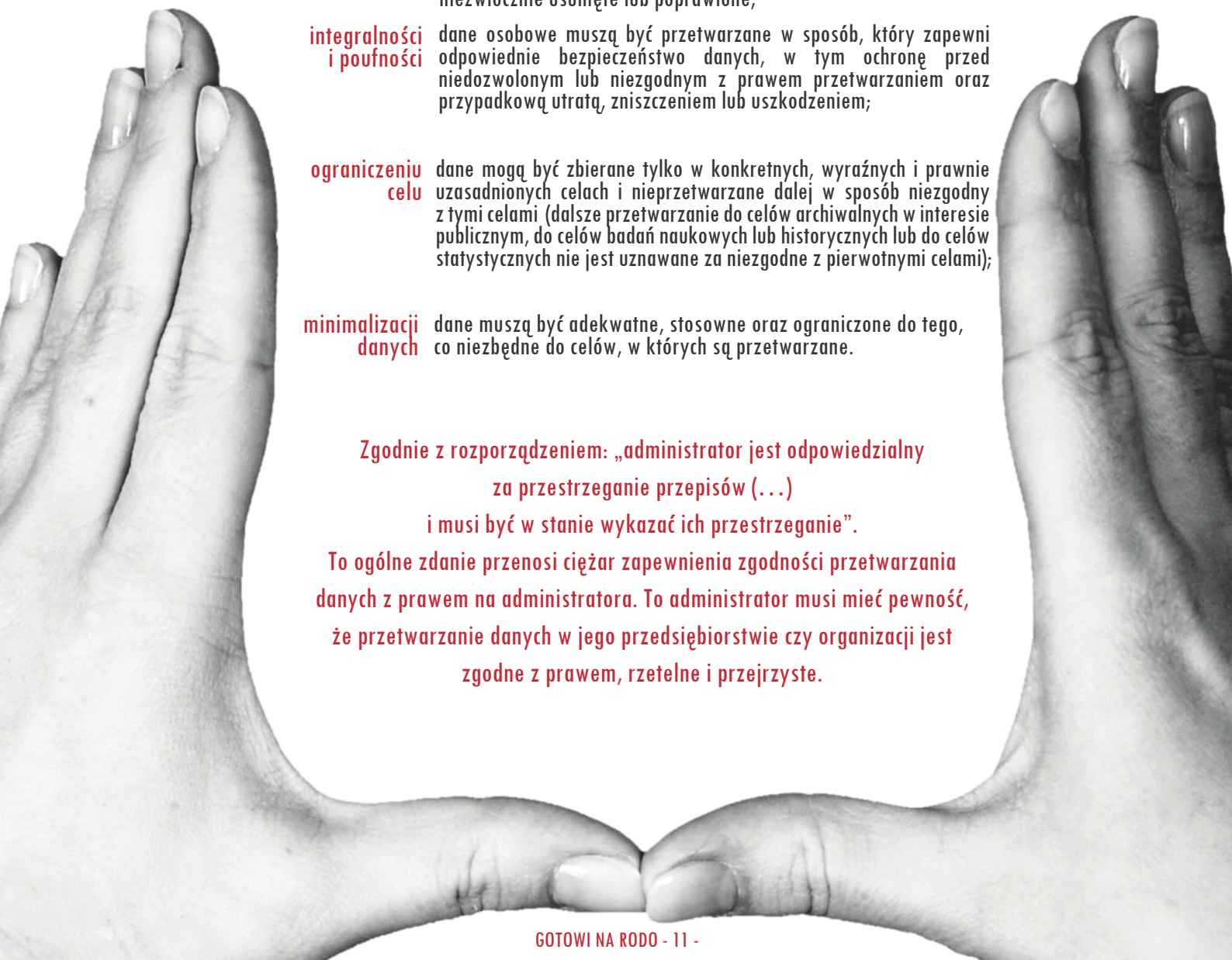
rozliczalności – administrator danych jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie;

prawidłowości – dane muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub poprawione;

integralności i poufności – dane osobowe muszą być przetwarzane w sposób, który zapewni odpowiednie bezpieczeństwo danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem;

ograniczeniu celu – dane mogą być zbierane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami);

minimalizacji danych – dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.



Zgodnie z rozporządzeniem: „administrator jest odpowiedzialny za przestrzeganie przepisów (...) i musi być w stanie wykazać ich przestrzeganie”. To ogólne zdanie przenosi ciężar zapewnienia zgodności przetwarzania danych z prawem na administratora. To administrator musi mieć pewność, że przetwarzanie danych w jego przedsiębiorstwie czy organizacji jest zgodne z prawem, rzetelne i przejrzyste.

3.4. ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

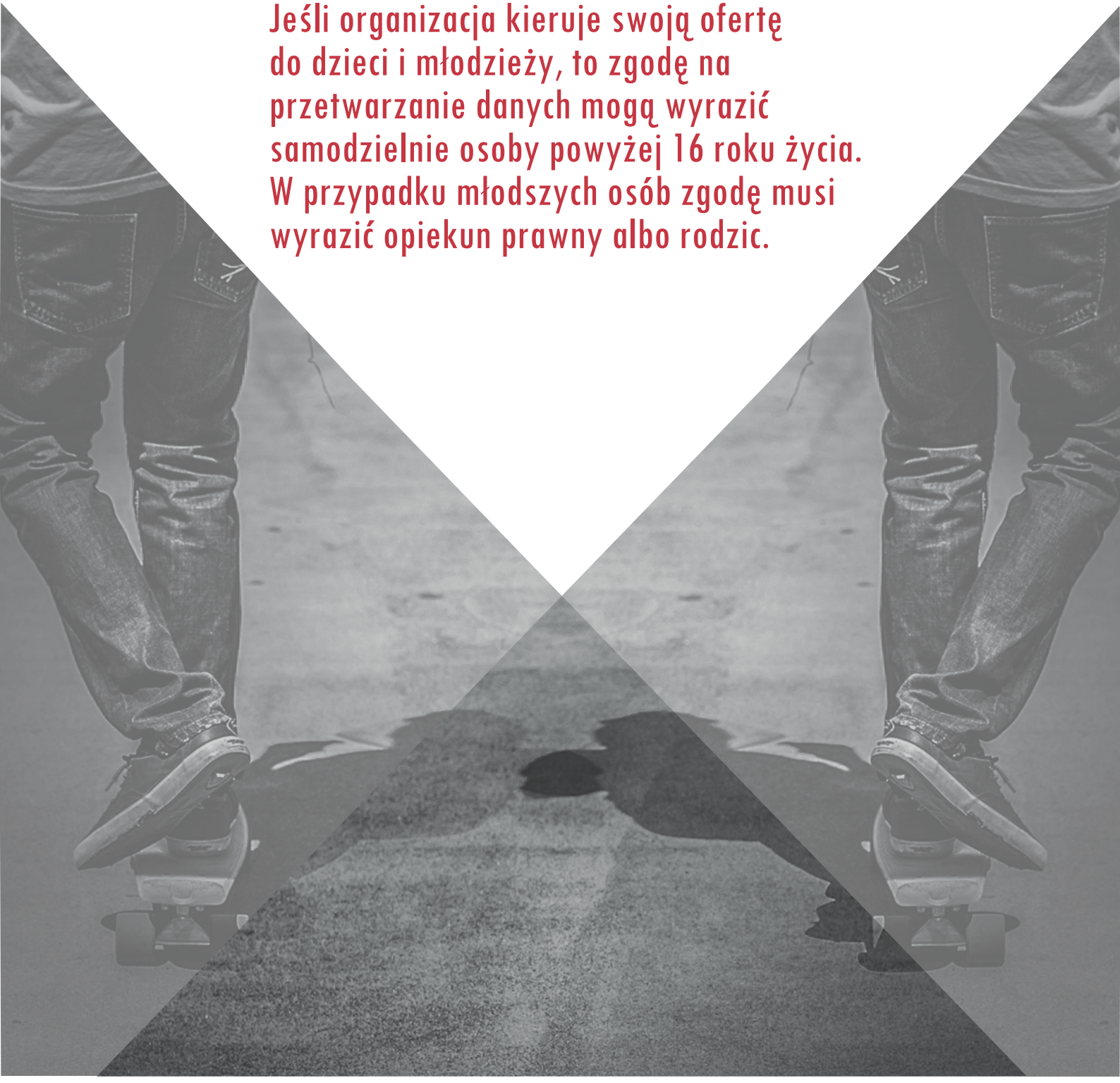
Przetwarzanie jest dozwolone wyłącznie jeżeli spełniony jest co najmniej jeden z poniższych warunków i wyłącznie w zakresie wynikającym z tego warunku:

zgoda osoby	np. wysyłka newslettera
ochrona żywotnych interesów osoby	np. monitorowanie epidemii
relizacja zadania w interesie osoby	np. zapobieganie skutkom klęski żywiołowej
prawnie uzasadniony interes	np. monitoring wizyjny
obowiązek wynikający z przepisów prawa	np. rekrutacja do pracy
czynności niezbędne do zawarcia lub wykonania umowy	np. ocena zdolności kredytowej

3.5. PRZETWARZANIE DANYCH NIELETNICH

W przypadku usług oferowanych bezpośrednio dziecku, np. w Internecie, zgodnie z prawem można przetwarzać dane osobowe dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaakceptowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

Jeśli organizacja kieruje swoją ofertę do dzieci i młodzieży, to zgodę na przetwarzanie danych mogą wyrazić samodzielnie osoby powyżej 16 roku życia. W przypadku młodszych osób zgodę musi wyrazić opiekun prawny albo rodzic.



3.6. SZCZEGÓLNA KATEGORIA DANYCH OSOBOWYCH

DANE SZCZEGÓLNIE WRAŻLIWE

ZACHOWAJ OSTROŻNOŚĆ !

RODO wprowadza zamknięty katalog szczególnych kategorii danych, których przetwarzanie jest zabronione poza sytuacjami wymienionymi w rozporządzeniu*.

Do takich danych zaliczamy:

pochodzenie rasowe lub etniczne;

poglądy polityczne;

przekonania religijne lub światopoglądowe;

przynależność do związków zawodowych.

A także przetwarzanie:

danych genetycznych;

danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej;

danych dotyczących zdrowia, seksualności lub orientacji seksualnej osoby fizycznej.

Są to tzw. dane wrażliwe. Organizacja może je przetwarzać tylko pod specjalnymi warunkami i musi się liczyć z koniecznością wdrożenia dodatkowych zabezpieczeń, takich jak np. szyfrowanie.

* Art. 9 ust. 2, 3, 4 RODO

3.7. AUTOMATYCZNE PRZETWARZANIE DANYCH

Automatyczne przetwarzanie danych w celu podjęcia decyzji – tzw. profilowanie – jest coraz bardziej powszechnym zjawiskiem. Marketing i branża reklamowa, bankowość, ubezpieczenia, ochrona zdrowia – to tylko niektóre z sektorów, gdzie korzysta się z operacji profilowania.

Profilowanie pomaga w analizie i wyciąganiu wniosków z zebranych danych. Jednak osoby, których dane dotyczą, często nie wiedzą, że ich dane są w ten sposób przetwarzane. Nie mogą więc korzystać ze swoich praw i np. kwestionować trafności takich działań. A jeśli konkretnej osobie zostaną przypisane nieprawidłowe cechy, może to doprowadzić do tego, że przetwarzane dane są po prostu niepoprawne.

Dlatego RODO w szczególny sposób reguluje operacje przetwarzania przy użyciu technik profilowania, w sytuacji kiedy to przetwarzanie:

- jest zautomatyzowane;
- dotyczy danych osobowych;
- ma na celu analizę efektów pracy osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Każda osoba, której dane dotyczą, ma prawo, by nie podlegać decyzjom, które opierają się na przetwarzaniu zautomatyzowanym – w tym profilowaniu, wywołującym dla tej osoby określone skutki prawne (np. brak możliwości udzielenia kredytu).

Dlatego rozporządzenie wyraźnie wskazuje sytuacje, w których profilowanie jest możliwe, tj.:
- przepis prawa na to zezwala;
- osoba, której dane dotyczą, udzieliła wyraźnej zgody.

W każdym z powyższych przypadków administrator danych powinien wdrożyć środki techniczne i organizacyjne, które zapewnią właściwe i bezpieczne przetwarzanie danych z wykorzystaniem profilowania. Zwłaszcza, jeśli do profilowania używa się szczególnych kategorii danych osobowych (danych wrażliwych) lub danych osobowych dzieci. Mają tu zastosowanie również wszystkie zasady przetwarzania danych (jak zasada adekwatności czy ograniczonego celu).

Przede wszystkim należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o jego konsekwencjach, a w szczególności o zasadach podejmowania decyzji. Pamiętać należy także o możliwości złożenia przez osobę fizyczną – w dowolnym momencie i bezpłatnie – sprzeciwu wobec przetwarzania danych, szczególnie jeśli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego. Kolejnym obowiązkiem jest przeprowadzenie oceny skutków dla ochrony danych dla operacji wykorzystujących profilowanie.

Jeśli wykorzystujesz zautomatyzowane systemy do podejmowania decyzji wobec osób fizycznych (w tym do ich profilowania), zwróć szczególną uwagę na obowiązki, których spełnienie będziesz musiał wykazać od 25 maja 2018 r. Szczególną uwagę poświęć analizie tego, jak wypełnisz obowiązki informacyjne wobec osób, które profilujesz.

3.8. PRZEKAZYWANIE DANYCH - PRZETWARZANIE W CHMURZE

Administratorzy danych coraz częściej decydują się na przekazanie danych osobowych innym firmom lub organizacjom, które w ich imieniu wykonują część operacji przetwarzania. Coraz popularniejsze są np. rozwiązania chmurowe. Administrator – aby wykorzystać możliwości obliczeniowe chmury – decyduje się na powierzenie procesu przetwarzania danych firmie zewnętrznej świadczącej tego rodzaju usługę.

W takich sytuacjach ważne jest, by podpisując umowę powierzenia danych osobowych, nie stracić nad nimi kontroli. Nie można dopuścić do sytuacji, w której powierzone dane będą wykorzystywane w innym celu, niż ten określony przez administratora.

Pamiętaj więc, aby powierzając przetwarzanie danych firmie zewnętrznej, korzystać wyłącznie z usługodawców, którzy mają odpowiednią wiedzę fachową, wiarygodność i zasoby.

Dotyczy to szczególnie gwarancji wdrożenia środków technicznych i organizacyjnych, które spełniają wymogi RODO, w tym wymogi bezpieczeństwa przetwarzania.

Przy wyborze można kierować się np. tym, czy firma posiada odpowiednie certyfikaty wydane na podstawie rozporządzenia.

W stosunku do dotychczasowych regulacji ważną zmianą jest to, że na firmie przetwarzającej spoczywają bardzo podobne obowiązki jak na administratorze danych. Przede wszystkim firma przetwarzająca musi wdrożyć środki techniczne i organizacyjne odpowiednie do ryzyk przetwarzania – tak by to przetwarzanie odpowiadało wymogom rozporządzenia.

Wśród innych obowiązków podmiotu przetwarzającego można wskazać:

- prowadzenie rejestru kategorii czynności przetwarzania;
- zgłaszanie naruszeń ochrony danych do administratora danych;
- wyznaczenie inspektora ochrony danych.

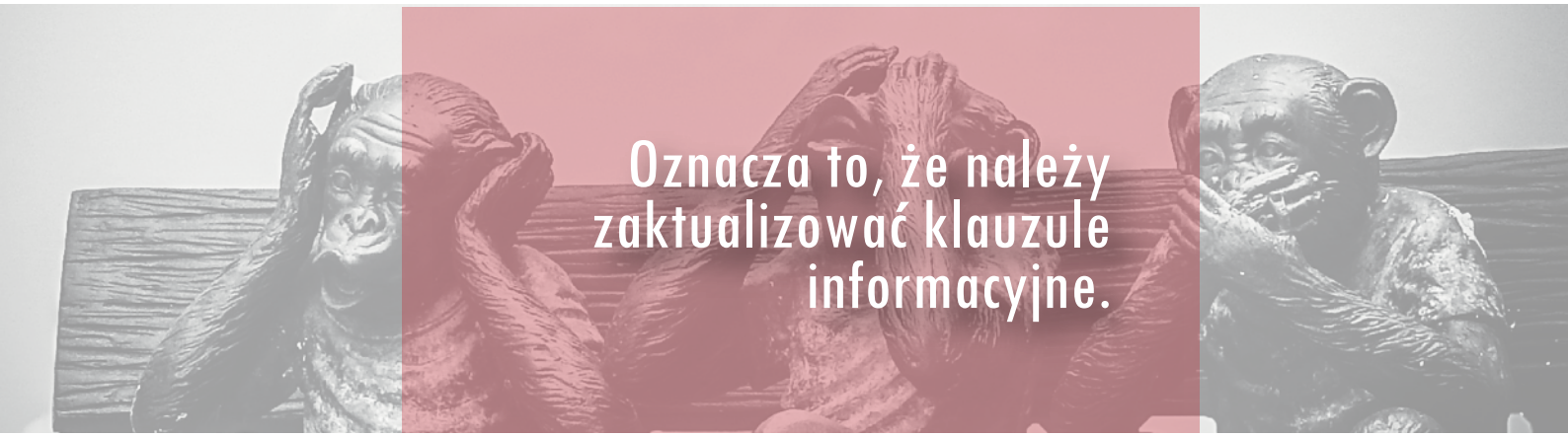
Powierzenie danych powinno być regulowane umową lub innym dokumentem, który określi:

- przedmiot i czas trwania przetwarzania
- charakter i cele przetwarzania
- rodzaj danych osobowych
- kategorie osób, których dane dotyczą
- konkretne zadania i obowiązki firmy przetwarzającej w związku z planowanym przetwarzaniem
- ryzyko naruszenia praw lub wolności osób fizycznych.

Jeżeli powierzasz przetwarzanie danych firmom lub organizacjom zewnętrznym, zachęcamy do przeglądu zawartych przez Twoją organizację umów powierzenia. Upewnij się, że podmiot, któremu powierzyłeś dane, będzie spełniał wszystkie określone w rozporządzeniu wymagania, zaś sama umowa zawiera wszelkie niezbędne elementy.

4. OBOWIĄZKI ORGANIZACJI JAKO ADMINISTRATORA DANYCH OSOBOWYCH
4.1. OBOWIĄZEK INFORMACYJNY

RODO wprowadza nowy katalog informacji jakie należy podać osobie, której dane dotyczą. Jest on dużo szerszy niż dotychczas.



Oznacza to, że należy zaktualizować klauzule informacyjne.

Ponadto, jeżeli administrator planuje przetwarzać dane osobowe w innym celu niż ten, w którym dane osobowe zostały zebrane, powinien poinformować osobę, której dane dotyczą, o tym innym celu oraz udzielić jej pozostałych stosownych informacji. Informacje powinny zostać podane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

Zgodnie z nowymi przepisami należy poinformować o:

danych organizacji, w tym danych kontaktowych i informacji o przedstawicielu jeśli jest;

danych kontaktowych inspektora ochrony danych;

celu przetwarzania danych i podstawie prawnej;

odbiorcach danych lub kategorii odbiorców jeśli występują;

zamiarze przekazania danych osobowych do państwa trzeciego (gdy ma to zastosowanie – informacje);

okresie przechowywania danych;

prawie osoby do żądania informacji, prawie do cofnięcia zgody i sposobie w jaki można to zrobić, prawie do wniesienia skargi do organu nadzorczego;

tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

4.2. OCENA SKUTKÓW DLA OCHRONY DANYCH

RODO nakłada obowiązek wdrożenia odpowiednich środków ochrony danych osobowych na administratorów. Administratorzy muszą też być w stanie wykazać przestrzeganie rozporządzenia pod kątem ryzyka naruszenia praw lub wolności osób fizycznych.

Ryzyko jest scenariuszem opisującym zdarzenie i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa wystąpienia.

Zarządzanie ryzykiem można natomiast określić jako działania mające na celu kierowanie organizacją i kontrolowanie organizacji pod kątem ryzyka.

Jak wspomniano wcześniej, nowe przepisy nie wymagają zgłaszania zbiorów danych osobowych do organu nadzorczego w celu rejestracji, co jest dużym ułatwieniem dla organizacji. Wymóg ten został natomiast zastąpiony obowiązkiem przeprowadzenia tzw. oceny skutków dla ochrony danych.

Ocena ta powinna dotyczyć przede wszystkim planowanych operacji i celów przetwarzania oraz zabezpieczeń i sposobów minimalizowania ryzyka. Ocena obejmuje dokumentację operacji przetwarzania danych, oceny niezbędności i proporcjonalności przetwarzania, ma także pomóc we właściwym zarządzaniu ryzykami wynikającymi z przetwarzania danych.

Zgodnie z przewidzianym w RODO podejściem opartym na analizie ryzyka, przeprowadzenie oceny skutków dla ochrony danych nie jest obowiązkowe dla każdej operacji przetwarzania. Wymaga się go wyłącznie w przypadku, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, np. w sytuacji:

- kiedy działania na danych dokonywane są przy użyciu nowych technologii;
- użycia zautomatyzowanych procesów przetwarzania danych, w tym profilowania;
- przetwarzania na dużą skalę szczególnych kategorii danych (danych wrażliwych, takich jak dane biometryczne czy dane na temat stanu zdrowia).

Jeśli administrator danych nie może wystarczająco zniwelować danego ryzyka lub mimo zastosowania środków ryzyko nadal jest wysokie, konieczna jest konsultacja z GIODO. Tego typu ocena musi się więc pojawić na etapie projektowania przetwarzania – jej wynik prowadzi bowiem do decyzji, czy przetwarzanie danych w zakładany sposób wymagać będzie uprzedniej konsultacji z GIODO. Rozporządzenie przewiduje też, że w określonych przypadkach konieczne może być konsultowanie zamiaru przetwarzania danych osobowych z osobami, których dane dotyczą lub ich przedstawicielami – np. poprzez formalne pytanie do przedstawicieli pracowników czy też badanie przesłane klientom.

Generalny Inspektor Ochrony Danych Osobowych przygotował propozycję wykazu rodzajów przetwarzania, dla których – zgodnie z art. 35 ust. 4 RODO – wymagane jest przeprowadzenie oceny skutków dla ochrony danych. Uruchomił też publiczne konsultacje w tym zakresie, aby zapewnić administratorom i podmiotom przetwarzającym lepsze przygotowanie się do stosowania RODO.

Wykaz powinien pomóc administratorom w podjęciu decyzji dotyczących przeprowadzenia oceny skutków.*

Nawet jeśli z oceny ryzyka nie wynika obowiązek przeprowadzenia oceny skutków dla ochrony danych, nie zmniejsza to obowiązku wdrożenia przez administratorów środków, które umożliwią odpowiednie zarządzanie ryzykiem naruszenia praw i wolności osób fizycznych.

W praktyce oznacza to, że administratorzy muszą stale oceniać ryzyko powodowane przez czynności przetwarzania, w celu określenia, kiedy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Zwłaszcza jeśli zmieniają się cele przetwarzania, zakres albo wykorzystane rozwiązania technologiczne.

Administratorzy danych powinni traktować przeprowadzenie oceny skutków dla ochrony danych jako przydatne i pozytywne działanie, które przyczynia się do zachowania zgodności z prawem.

* Informacja o konsultacjach dostępna pod adresem: https://giodo.gov.pl/pl/1520281/10430.

4. OBOWIĄZKI ORGANIZACJI JAKO ADMINISTRATORA DANYCH OSOBOWYCH
4.2. OCENA SKUTKÓW DLA OCHRONY DANYCH

Kiedy przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe?

O ile operacja przetwarzania nie stanowi wyjątku*, ocenę skutków dla ochrony danych należy przeprowadzić wówczas, gdy operacja przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Operacja przetwarzania może powodować wysokie ryzyko w szczególności w przypadku:

- systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
- przetwarzania na dużą skalę szczególnych kategorii danych osobowych, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa lub;
- systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

* Zgodnie z art. 35 ust. 5 i 10 Rozporządzenia, z wyjątkiem mamy do czynienia, gdy spełniony jest jeden z warunków:
- organ nadzorczy ustanowił i podał do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych
- przetwarzanie ma podstawę prawną w prawie Unii lub państwa członkowskiego i prawo takie reguluje daną operację przetwarzania (lub zestaw operacji), a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji przed przyjęciem tej podstawy prawnej).

Przy określaniu operacji przetwarzania, które mogą powodować wysokie ryzyko, należy wziąć pod uwagę dziewięć kryteriów:

Ocena lub punktacja, w tym profilowanie i prognozowanie, w szczególności w zakresie efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą;

Przykład: instytucja finansowa sprawdza swoich klientów w bazie danych kredytowych; przedsiębiorstwo biotechnologiczne bezpośrednio oferuje klientom badania genetyczne w celu oceny i prognozowania ryzyka wystąpienia choroby lub zagrożeń dla zdrowia; organizacja tworzy profile zachowań lub profile marketingowe w oparciu o nawigację na swojej stronie internetowej.

Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku: przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, wywołujące skutki prawne wobec tych osób. Przykładowo, przetwarzanie może prowadzić do wykluczenia lub dyskryminacji osób fizycznych. Przetwarzanie, które ma niewielki wpływ na osoby fizyczne lub nie ma na nie żadnego wpływu, nie spełnia tego konkretnego kryterium;

Przykład: Systemy profilowania klientów pod kątem preferencji zakupowych, ustalanie cen promocyjnych w oparciu o profil.

Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub w ramach systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie;

Przykład: Gromadzenie i wykorzystywanie danych przez aplikacje instalowane w urządzeniach mobilnych, w tym ubieralnych (wereable devices).

Dane wrażliwe lub dane o charakterze wysoce osobistym: szczególne kategorie danych osobowych oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa;

Przykład: Szpital przechowujący dokumentację medyczną pacjentów lub prywatny detektyw przechowujący szczegółowe dane przestępców.

4.2. OCENA SKUTKÓW DLA OCHRONY DANYCH

Oprócz kategorii wymienionych w przepisach, niektóre kategorie danych można uznać za zwiększające potencjalne ryzyko naruszenia praw i wolności osób fizycznych:

- dane powiązane z gospodarstwem domowym i działalnością prywatną (taką jak łączność elektroniczna, której poufność należy chronić);
- dane dotyczące lokalizacji, których gromadzenie jest sprzeczne ze swobodą poruszania się;
- dane finansowe, które mogą zostać wykorzystane do oszustw płatniczych;
- dokumenty osobiste;
- wiadomości e-mail;
- pamiętniki;
- notatki z e-czytników wyposażonych w funkcję notatnika;
- dane mające bardzo osobisty charakter zawarte w aplikacjach rejestrujących codzienną aktywność.

Dane przetwarzane na dużą skalę: RODO nie określa, co to znaczy przetwarzanie na dużą skalę. Aby stwierdzić czy przetwarzanie danych odbywa się na dużą skalę, należy wziąć pod uwagę następujące czynniki:

a. liczbę osób, których dane dotyczą
b. ilość danych lub zakres poszczególnych pozycji danych
c. czas trwania lub trwałość czynności przetwarzania danych
d. zakres geograficzny czynności przetwarzania.

Dopasowywanie lub łączenie zbiorów danych, np. pochodzących z co najmniej dwóch operacji przetwarzania przeprowadzonych w różnych celach lub przez różnych administratorów, w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.

Przykład: Łączenie danych z różnych rejestrów państwowych i/lub publicznych przez firmy marketingowe w celach przeprowadzania akcji marketingowych ukierunkowanych na określone grupy klientów.

Dane dotyczące osób wymagających szczególnej opieki, do których zaliczają się:

- dzieci
- pracownicy
- wrażliwe grupy społeczne wymagające szczególnej ochrony:
  - osoby chore psychicznie
  - osoby ubiegające się o azyl
  - osoby starsze
  - pacjenci itp.

Przykład: Systemy służące do zgłaszania nieprawidłowości (związanych np. z korupcją, mobbingiem) – w szczególności, gdy przetwarzane są w nim dane pracowników.

Stosowanie nowych rozwiązań technologicznych lub organizacyjnych albo ich innowacyjne wykorzystanie.

Przykład: Połączenie technologii rozpoznających odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu.

Przetwarzanie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy. Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom fizycznym dostępu do usługi lub zawarcia umowy, zmiana tej usługi lub odmowa jej wykonania.

Przykład: sytuacja, w której bank sprawdza klienta w bazie danych kredytowych, aby zdecydować, czy udzielić mu kredytu.

4.2. OCENA SKUTKÓW DLA OCHRONY DANYCH

przykład przetwarzania	ewentualne istotne kryteria	czy istnieje prawdopodobieństwo, że wymagane będzie przeprowadzenie oceny skutków dla ochrony danych?
Organizacja działa w obszarze ochrony zdrowia, prowadzi terapię i rehabilitację.	Dane wrażliwe lub dane o charakterze wysoce osobistym. Dane dotyczące osób wymagających szczególnej opieki. Dane przetwarzane na dużą skalę.	TAK
Zastosowanie systemu kamer monitorujących zachowanie kierowców na drogach. Administrator planuje wykorzystać inteligentny system analizy obrazu do namierzania pojedynczych samochodów i automatycznego rozpoznawania tablic rejestracyjnych.	Systematyczne monitorowanie. Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych.	TAK
Przedsiębiorstwo systematycznie monitoruje działania swoich pracowników: stanowiska pracy i aktywność w internecie itd.	Systematyczne monitorowanie. Dane dotyczące osób wymagających szczególnej opieki.	TAK
Organizacja gromadzi publiczne dane z mediów społecznościowych w celu wygenerowania profilu.	Ocena lub punktacja. Dane przetwarzane na dużą skalę. Dopasowanie lub łączenie zbiorów danych. Dane wrażliwe lub dane o charakterze wysoce osobistym.	TAK
Instytucja tworząca krajowy rating kredytowy lub bazę danych zawierającą informacje o nadużyciach finansowych.	Ocena lub punktacja. Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku. Uniemożliwienie osobom, których dane dotyczą, wykonywania prawa lub korzystania z usługi lub umowy. Dane wrażliwe lub dane o charakterze wysoce osobistym.	TAK
Organizacja przechowuje do celów archiwizacji wrażliwe dane osobowe opatrzone pseudonimem, dotyczące osób wymagających szczególnej opieki, biorących udział w projektach badawczych.	Dane wrażliwe. Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą. Uniemożliwienie osobom, których dane dotyczą, wykonywania prawa lub korzystania z usługi lub umowy. Dane wrażliwe lub dane o charakterze wysoce osobistym.	TAK
Przetwarzanie danych osobowych pacjentów lub klientów przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika	Dane wrażliwe lub dane o charakterze wysoce osobistym. Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą.	TAK
Organizacja korzysta z listy dystrybucyjnej do wysyłania ogólnego newslettera do swoich subskrybentów	Dane przetwarzane na dużą skalę.	NIE
Strona internetowa z handlem elektronicznym wyświetla reklamy części do samochodów i korzysta z ograniczonego profilowania w oparciu o elementy przeglądane lub kupione na tej stronie.	Ocena lub punktacja.	NIE

Przykładowo, przetwarzanie danych dotyczących zdrowia na dużą skalę uważa się za mogące powodować wysokie ryzyko i wymaga ono przeprowadzenia oceny skutków dla ochrony danych. W takim przypadku obowiązkiem administratora danych jest dokonanie oceny ryzyka naruszenia praw i wolności osób fizycznych oraz określenie, jakie środki zaplanować w celu zmniejszenia ryzyka do dopuszczalnego poziomu i wykazania przestrzegania RODO.

Przykładem zmniejszenia ryzyka, jeżeli chodzi o przechowywanie danych osobowych na laptopach, może być zastosowanie odpowiednich technicznych i organizacyjnych środków bezpieczeństwa (skuteczne szyfrowanie całego dysku, solidne zarządzanie kluczami, odpowiednia kontrola dostępu, zabezpieczone kopie zapasowe, itd.), które uzupełnią już stosowane środki. W przypadkach, w których nie jest jasne, czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych, zaleca się przeprowadzenie takiej oceny, ponieważ stanowi ona przydatne narzędzie ułatwiające administratorom przestrzeganie RODO.

4.2. OCENA SKUTKÓW DLA OCHRONY DANYCH

Kiedy przeprowadzenie oceny skutków dla ochrony danych **NIE JEST** obowiązkowe?

Ocena skutków dla ochrony danych nie jest wymagana w następujących przypadkach:

gdy nie jest prawdopodobne, aby operacja przetwarzania mogła powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;

gdy charakter, zakres, kontekst i cele przetwarzania są bardzo podobne do operacji przetwarzania, w przypadku których przeprowadzono już ocenę skutków dla ochrony danych. W takich przypadkach można wykorzystać wyniki wcześniej przeprowadzonej oceny skutków dla ochrony danych;

gdy operacje przetwarzania zostały sprawdzone przez organ nadzorczy przed majem 2018 r. w szczególnych warunkach, które nie uległy zmianie;

jeżeli operacja przetwarzania ma podstawę prawną w prawie UE lub w prawie państwa członkowskiego, które reguluje daną operację przetwarzania, oraz jeżeli oceny skutków dla ochrony danych dokonano już w związku z przyjęciem tej podstawy prawnej;

jeżeli operacje przetwarzania zostały umieszczone w utworzonym przez organ nadzorczy wykazie operacji, które nie podlegają wymogowi przeprowadzenia oceny skutków dla ochrony danych. W takich przypadkach, o ile wykaz ten nie ulegnie zmianie, przeprowadzenie oceny skutków dla ochrony danych nie jest wymagane, ale tylko wtedy, gdy przetwarzanie jest ściśle zgodne z wykazem i z wymogami RODO.

A co z już istniejącymi operacjami przetwarzania?

W pewnych okolicznościach wymagane jest przeprowadzenie ocen skutków dla ochrony danych dla już istniejących operacji przetwarzania. Dotyczy to tych operacji, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Dotyczy także sytuacji, kiedy nastąpiła zmiana rodzaju ryzyka.

Ponadto przeprowadzenie oceny skutków dla ochrony danych może być wymagane po zmianie rodzaju ryzyka operacji przetwarzania, np. z powodu wykorzystania nowej technologii lub dlatego, że dane osobowe wykorzystywane są w innym celu. Operacje przetwarzania danych mogą się szybko zmieniać i mogą pojawić się nowe zagrożenia.

Przeprowadzenie oceny skutków dla ochrony danych może być również konieczne ze względu na zmianę kontekstu organizacyjnego lub społecznego czynności przetwarzania, np. ponieważ skutki niektórych automatycznie podejmowanych decyzji stały się bardziej znaczące lub ponieważ nowe kategorie osób fizycznych są narażone na dyskryminację. Każdy z tych przykładów może być elementem prowadzącym do zmiany ryzyka danej czynności przetwarzania.

Z drugiej strony, niektóre zmiany mogą również zmniejszyć ryzyko. Na przykład operacja przetwarzania może ewoluować w taki sposób, że decyzje nie będą już podejmowane automatycznie, lub działania monitorujące przestaną być realizowane systematycznie. W tym przypadku przegląd przeprowadzonej analizy ryzyka może wykazać, że nie ma już potrzeby przeprowadzenia oceny skutków dla ochrony danych.

Dobrą praktyką jednak powinno być stałe przeprowadzanie przeglądu oceny skutków dla ochrony danych i regularne przeprowadzanie ponownej oceny. W związku z tym, nawet jeżeli w dniu 25 maja 2018 r. nie wymaga się przeprowadzenia oceny skutków dla ochrony danych, administrator będzie musiał w odpowiednim momencie przeprowadzić taką ocenę w ramach swoich ogólnych obowiązków w zakresie rozliczalności, jeśli spełnione zostaną przesłanki wskazane w art. 35 RODO.

4.2. OCENA SKUTKÓW DLA OCHRONY DANYCH

W jakim momencie należy przeprowadzić ocenę skutków dla ochrony danych?

Przed rozpoczęciem przetwarzania.

Jest to zgodne z zasadami dotyczącymi uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych. Ocenę skutków dla ochrony danych należy traktować jako narzędzie wspomagające podejmowanie decyzji w sprawie przetwarzania danych.

Ocena skutków dla ochrony danych powinna rozpocząć się jak najwcześniej w fazie projektowania operacji przetwarzania, nawet jeżeli niektóre operacje przetwarzania jeszcze są nieznane. W miarę rozwoju procesu konieczne może być również powtórzenie poszczególnych etapów oceny, ponieważ wybór niektórych środków technicznych lub organizacyjnych może wpłynąć na prawdopodobieństwo wystąpienia zagrożenia lub jego wagę.

Fakt, że aktualizacja oceny skutków dla ochrony danych może okazać się konieczna już po rozpoczęciu przetwarzania, nie uzasadnia odroczenia lub nieprzeprowadzenia oceny skutków dla ochrony danych. Ocena skutków dla ochrony danych jest procesem ciągłym, szczególnie gdy operacja przetwarzania podlega zmianom.

Prowadzenie oceny skutków dla ochrony danych powinno być procesem ciągłym, a nie jednorazowym.

Kto jest zobowiązany do przeprowadzenia oceny skutków dla ochrony danych?

Administrator, wspólnie z IOD-em i ewentualnie firmą przetwarzającą.

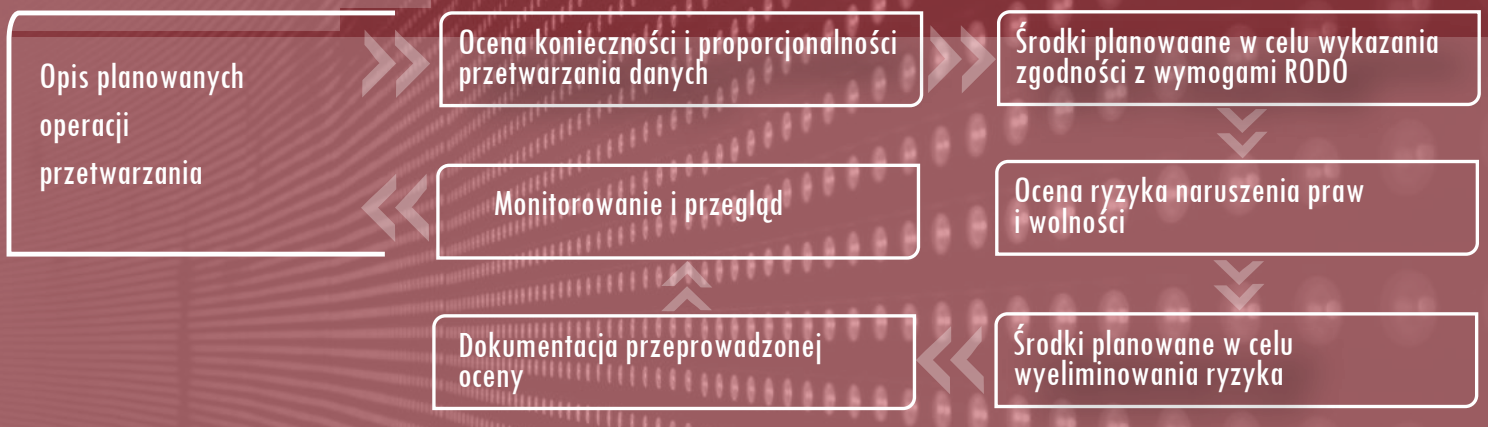
Za zapewnienie przeprowadzenia oceny skutków dla ochrony danych jest odpowiedzialny administrator. Ocenę skutków dla ochrony danych można powierzyć firmie zewnętrznej, jednak ostateczna odpowiedzialność za wykonanie zadania spoczywa na administratorze. W niektórych przypadkach administrator musi zasięgnąć opinii osób, których dane dotyczą, lub ich przedstawicieli (np. związków zawodowych).

Co powinna zawierać ocena skutków dla ochrony danych?

RODO określa minimalne elementy oceny skutków dla ochrony danych:

- opis planowanych operacji przetwarzania i celów przetwarzania;
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne;
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- środki planowane w celu:
  - zaradzenia ryzyku;
  - wykazania przestrzegania rozporządzenia.

Na poniższym wykresie przedstawiono standardowy, powtarzalny proces przeprowadzania oceny skutków dla ochrony danych:



4.2. OCENA SKUTKÓW DLA OCHRONY DANYCH

Z perspektywy zarządzania ryzykiem ocena skutków dla ochrony danych ma na celu zarządzanie czynnikami ryzyka naruszenia praw i wolności osób fizycznych, poprzez:

określanie kontekstu: uwzględnienie charakteru, zakresu i celów przetwarzania oraz źródeł ryzyka;

przeprowadzanie oceny ryzyka: ocena konkretnego prawdopodobieństwa i powagi tego wysokiego ryzyka;

traktowanie ryzyka: minimalizowanie tego ryzyka i zapewnienie ochrony danych osobowych, a także wykazanie przestrzegania niniejszego rozporządzenia.

Metody przeprowadzania oceny skutków dla ochrony danych

Można zastosować różne metodyki ochrony danych i oceny skutków, aby wspomóc wdrażanie podstawowych wymogów określonych w RODO.
W załączniku 1 znajdują się wspólne kryteria, które mają umożliwić stosowanie różnych metod, a jednocześnie pozwolić administratorom na zachowanie zgodności z RODO. Kryteria te uściślają podstawowe wymogi zawarte w rozporządzeniu, ale dają też wystarczającą swobodę, aby umożliwić różne formy wdrażania. Kryteria można wykorzystać do wykazania, że konkretna metodyka oceny skutków dla ochrony danych spełnia standardy przewidziane w RODO. Decyzję o wyborze metodyki podejmuje administrator danych, lecz powinna ona być zgodna z kryteriami określonymi w załączniku 1.

W niektórych przypadkach ocena skutków może być skomplikowanym i kompleksowym procesem. Szczegółowe informacje dotyczące oceny skutków dla ochrony danych znajdują się w dokumencie opracowanym przez specjalną Grupę Roboczą Art. 29 Wytyczne dotyczące oceny skutków dla ochrony danych (WP 248).
Dokument dostępny jest na stronie:
www.giodo.gov.pl/Reforma

www.giodo.gov.pl/p/reforma-przepisow » Opinie i wytyczne Grupy Roboczej art. 29 » Przyjęte

Niezależnie od formy, ocena skutków dla ochrony danych musi stanowić rzeczywistą ocenę ryzyka, która pozwala administratorom podjąć działania na rzecz wyeliminowania ryzyka.

Uwaga: przy przeprowadzaniu oceny skutków dla ochrony danych przyjmujemy perspektywę osób fizycznych, ponieważ ocena dotyczy ryzyka naruszenia praw tych osób.

Niezależnie od formy, ocena skutków dla ochrony danych musi stanowić rzeczywistą ocenę ryzyka, która pozwala administratorom podjąć działania na rzecz wyeliminowania ryzyka.

4.3. UPRZEDNIE KONSULTACJE

Kiedy należy skonsultować się z organem nadzorczym?

Jeżeli ryzyko szczątkowe* jest wysokie.

Niedopuszczalne wysokie ryzyko szczątkowe obejmuje przypadki, w których osoby fizyczne mogą ponieść znaczne lub nawet nieodwracalne konsekwencje, z którymi nie będą mogły sobie poradzić (np.: bezprawne uzyskanie dostępu do danych prowadzące do zagrożenia życia osób, zwolnienie, zagrożenie o charakterze finansowym) lub w których wydaje się oczywiste, że wystąpi ryzyko (np.: ograniczenie liczby osób mających dostęp do danych nie jest możliwe ze względu na sposób ich udostępniania, wykorzystywania lub rozprowadzania lub gdy luka w zabezpieczeniach, o której istnieniu wiadomo, nie zostanie usunięta).

Zawsze gdy administrator danych nie może znaleźć środków wystarczających do zmniejszenia ryzyka do dopuszczalnego poziomu (np. ryzyko szczątkowe wciąż jest wysokie), wymagane są konsultacje z organem nadzorczym.

Jeżeli ocena skutków dla ochrony danych wykaże, że przetwarzanie spowoduje wysokie ryzyko, jeśli administrator nie zastosuje środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator powinien skonsultować się z organem nadzorczym. W przypadku organizacji mających siedzibę w Polsce jest to Urząd Ochrony Danych Osobowych – UODO. Należy wskazać: cele i sposoby zamierzonego przetwarzania, środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, ocenę skutków dla ochrony danych i dane kontaktowe inspektora ochrony danych (jeżeli został wyznaczony).

Informacje potrzebne w celu konsultacji:

- cele i sposoby zamierzonego przetwarzania
- środki i zabezpieczenia dla ochrony praw i wolności osób, których dane dotyczą
- dane kontaktowe inspektora ochrony danych
- ocena skutków dla ochrony danych

Ryzyko szczątkowe* – ryzyko, które pozostaje po zastosowaniu wszelkich możliwych środków bezpieczeństwa i przeprowadzeniu działań zmierzających do zminimalizowania ryzyka – nie można go wyeliminować.

4.4. REJESTRACJA CZYNNOŚCI PRZETWARZANIA

Każdy administrator powinien prowadzić wewnętrzny rejestr czynności przetwarzania danych osobowych, jeśli:

zatrudnia więcej niż 250 osób;

przetwarzanie, którego dokonuje, może powodować ryzyko naruszenia praw lub wolności osób których dane dotyczą;

przetwarzanie nie ma charakteru sporadycznego;

przetwarzanie obejmuje szczególne kategorie danych osobowych;

przetwarzane dane osobowe dotyczą wyroków skazujących i naruszeń prawa.

W rejestrze należy zamieścić następujące informacje:

imię i nazwisko lub nazwę oraz dane kontaktowe administratora;

imię i nazwisko inspektora ochrony danych;

cele przetwarzania;

opis kategorii osób, których dane dotyczą (np. kandydaci do pracy);

kategorię danych osobowych (np. dane adresowe, dane o przebiegu kariery zawodowej);

kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym w państwach trzecich;

planowane terminy usunięcia poszczególnych kategorii danych;

ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

UWAGA! Przestają obowiązywać dotychczasowe wymogi dotyczące dokumentacji (polityki bezpieczeństwa, instrukcje zarządzania systemem informatycznym) i rozwiązań technologicznych, jak również poziomów zabezpieczeń (trzy poziomy środków bezpieczeństwa – podstawowy, podwyższony, wysoki).

Zostały one zastąpione jedną zasadą rozliczalności. To administrator będzie musiał udowodnić, że sposób przetwarzania danych osobowych i wprowadzone zabezpieczenia są wystarczające w stosunku do danej kategorii danych i celu przetwarzania. Pomimo tego, że dotychczasowe wymogi nie będą już obowiązywać, w niektórych przypadkach wskazany w nich sposób ochrony będzie odpowiedni.

Po 25 maja 2018 r. całkowicie zostanie zniesiony obowiązek zgłaszania zbiorów danych do rejestracji przez organ nadzorczy, a zastąpi go prowadzony przez każdego administratora rejestr czynności przetwarzania.

4.5. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

Zgłoszenie naruszenia ochrony danych musi nastąpić w ciągu 72 godzin od momentu stwierdzenia tego naruszenia.

STWIERDZENIE NARUSZENIA »

» ZGŁOSZENIE NARUSZENIA DO ORGANU NADZORCZEGO MUSI ZAWIERAĆ CO NAJMNIEJ:

- opis charakteru naruszenia wraz z informacją o kategorii i przybliżonej liczbie osób, których dane dotyczą;
- kategorii danych, liczbie wpisów;
- dane kontaktowe inspektora ochrony danych;
- opis możliwych konsekwencji naruszenia;
- opis zastosowanych lub proponowanych środków zaradczych.

4.6. ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

NARUSZENIE, KTÓRE MOŻE POWODOWAĆ WYSOKIE RYZYKO NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH

NIEZWŁOCZNIE NALEŻY PRZEKAZAĆ OSOBIE, KTÓREJ DOTYCZĄ

dane kontaktowe inspektora ochrony danych;

opis możliwych konsekwencji naruszenia;

opis zastosowanych lub proponowanych środków zaradczych.

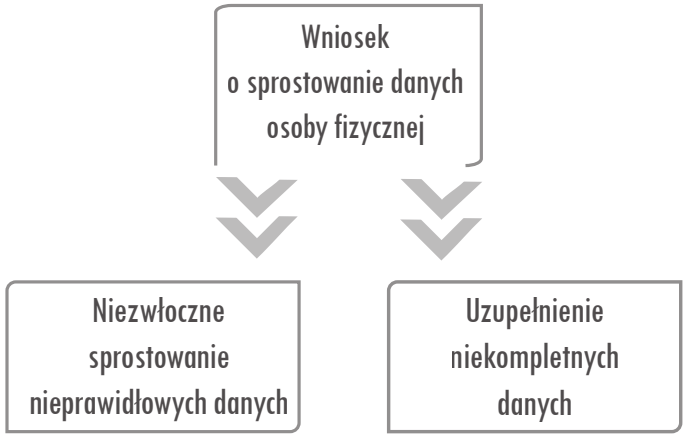
5. OBOWIĄZKI ADMINISTRATORA WYNIKAJĄCE Z PRAW OSÓB FIZYCZNYCH
5.1. PRAWO DOSTĘPU DO DANYCH
5.2. PRAWO SPROSTOWANIA DANYCH
5.3. PRAWO DO BYCIA ZAPOMNIANYM

PRAWO DOSTĘPU DO DANYCH

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są jej dane osobowe, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich w postaci kopii przetwarzanych danych, jak również do informacji dot. m.in. celu przetwarzania i okresu przechowywania danych. Złożenie wniosku w powyższym trybie powinno być bezpłatne, a administrator powinien odpowiedzieć na wniosek w ciągu miesiąca.

PRAWO SPROSTOWANIA DANYCH

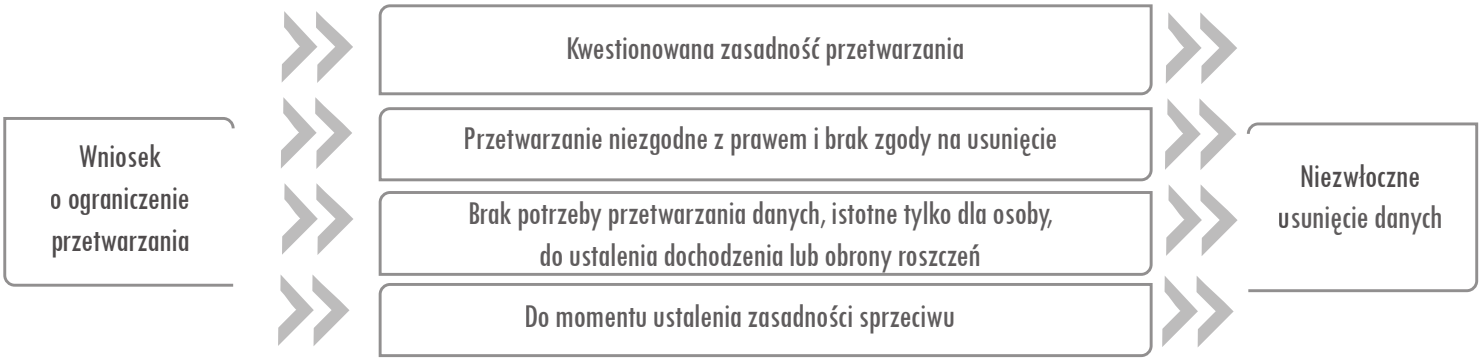
Osoba fizyczna ma prawo żądania od administratora niezwłocznego sprostowania swoich danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania osoba fizyczna ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.



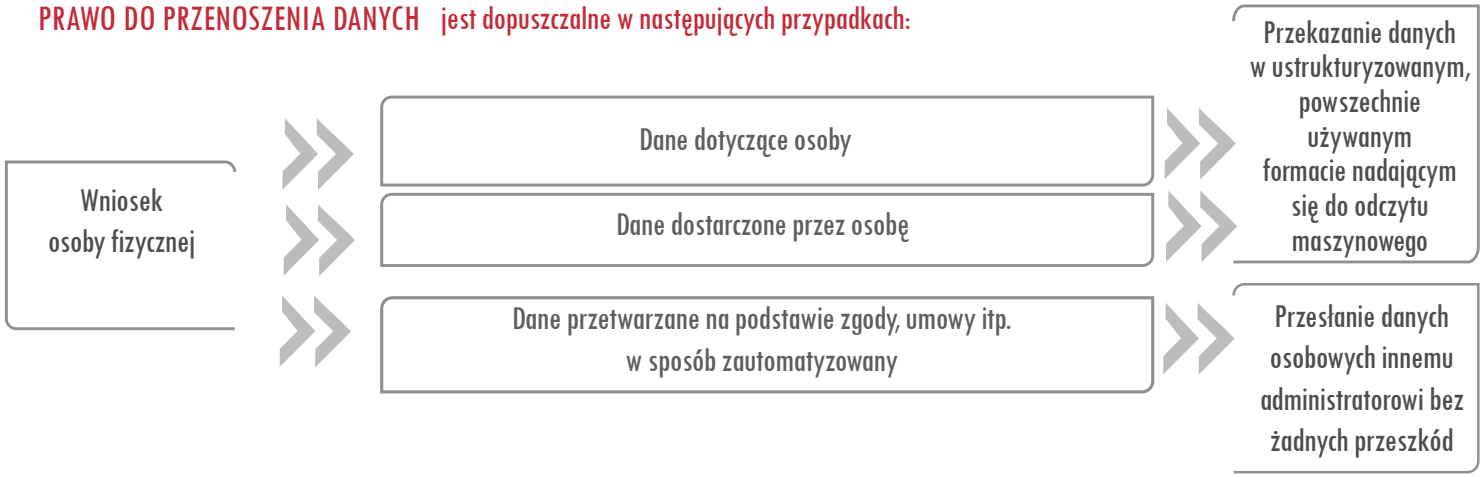
PRAWO DO BYCIA ZAPOMNIANYM jest dopuszczalne w następujących przypadkach:

5. OBOWIĄZKI ADMINISTRATORA WYNIKAJĄCE Z PRAW OSÓB FIZYCZNYCH
5.4. PRAWO DO OGRANICZENIA PRZETWARZANIA
5.5. PRAWO DO PRZENOSZENIA DANYCH
5.6. PRAWO DO SPRZECIWU

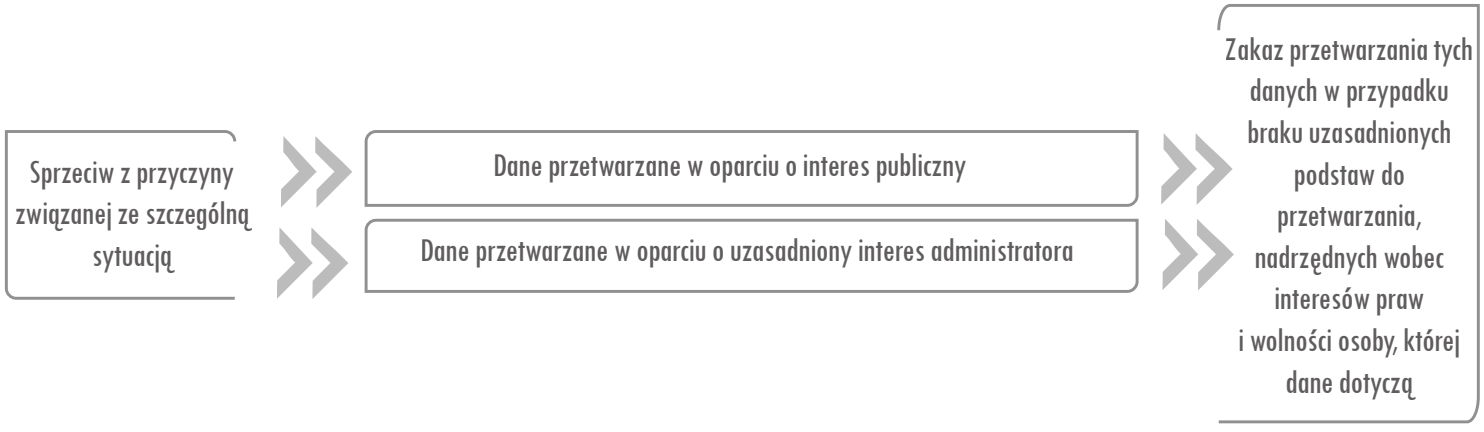
PRAWO DO OGRANICZENIA PRZETWARZANIA jest dopuszczalne w następujących przypadkach:



PRAWO DO PRZENOSZENIA DANYCH jest dopuszczalne w następujących przypadkach:



PRAWO DO SPRZECIWU jest dopuszczalne w następujących przypadkach:



6. INSPEKTOR OCHRONY DANYCH

IOD-em może być osoba posiadająca odpowiednie kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych. Tak jak w przypadku dotychczasowych ABI, funkcję tę może pełnić osoba zatrudniona u administratora albo zewnętrzny profesjonalista, a zadania IOD - a można łączyć z pełnieniem innych obowiązków.

Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy, a wypełniając swoje obowiązki IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

Inspektor Ochrony Danych (IOD), będący niejako następcą Administratora Bezpieczeństwa Informacji (ABI), musi zostać powołany między innymi gdy:

- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób na dużą skalę;
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Zachęcamy do zapoznana się z Wytycznymi opracowanymi przez Grupę Roboczą Art. 29 ds. Ochrony Danych: Wytyczne dotyczące inspektorów ochrony danych (WP 243). Dokument jest dostępny na stronie www.giodo.gov.pl

Zadania inspektora chrony danych:

informowanie o obowiązkach wynikających z RODO i innych przepisów;

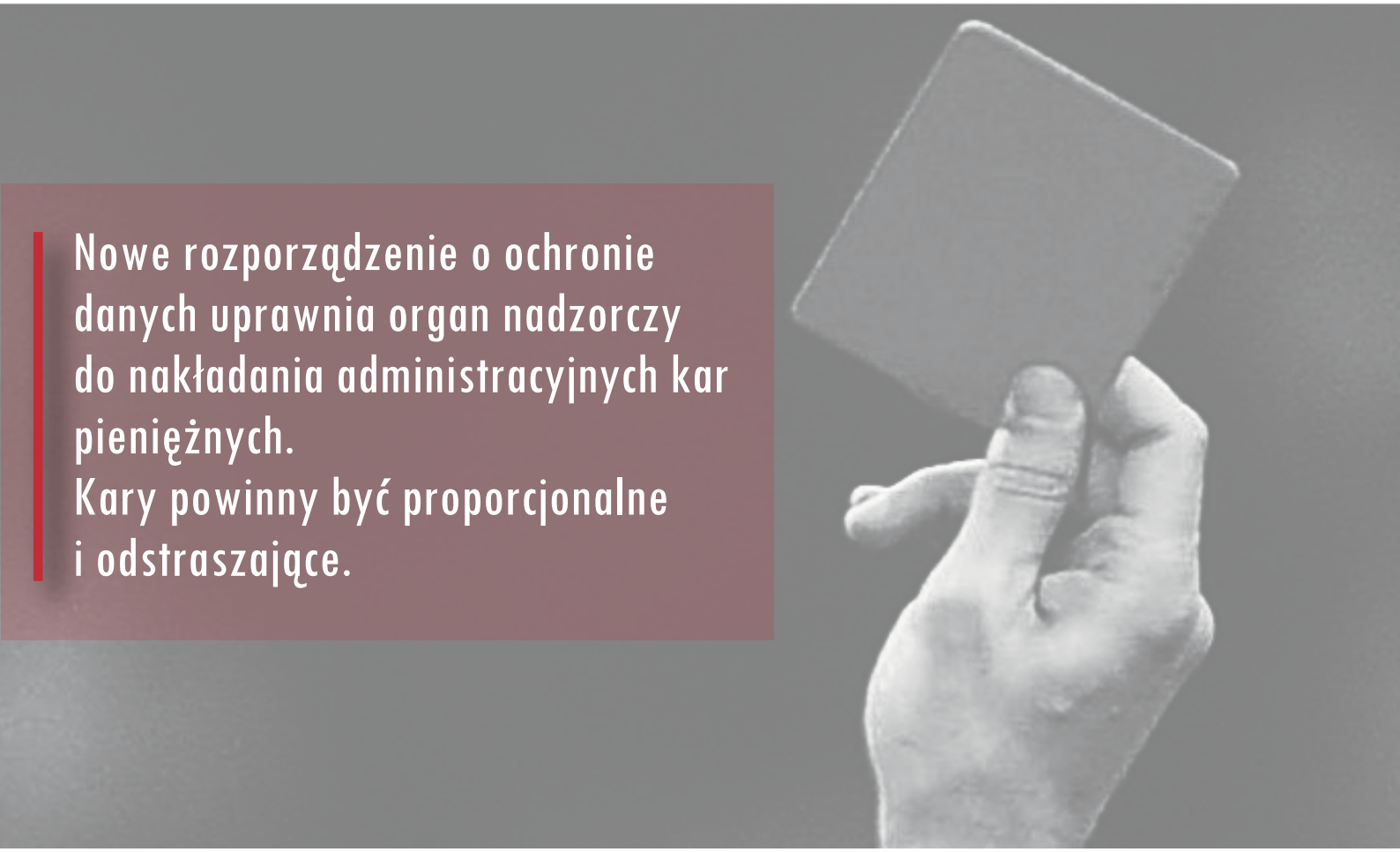
monitorowanie przestrzegania przez Administratora lub Przetwarzającego RODO i innych przepisów o ochronie danych osobowych przez administratora i przetwarzającego;

szkolenia i audyty;

udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

współpraca z organem nadzorczym i pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z tzw. uprzednimi konsultacjami.

7. SANKCJE



Nowe rozporządzenie o ochronie danych uprawnia organ nadzorczy do nakładania administracyjnych kar pieniężnych.
Kary powinny być proporcjonalne i odstraszające.

kara w wysokości
10 000 000 euro albo 2% całkowitego rocznego obrotu

Niezastosowanie się do warunków wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego*;

Nieuwzględnienie ochrony danych w fazie projektowania oraz domyślnej ochrony danych;

Nieprzestrzeganie przepisów dotyczących rejestrowania czynności przetwarzania;

Niedopełnienie obowiązków związanych z inspektorem ochrony danych.

kara w wysokości
20 000 000 euro albo 4% całkowitego rocznego obrotu

Naruszenie podstawowych zasad przetwarzania danych;

Naruszenie warunków wyrażenia zgody;

Naruszenie przepisów dotyczących przetwarzania szczególnej kategorii danych;

Niedopełnienie obowiązku informacyjnego;

Niedopełnienie obowiązków wynikających z prawa dostępu, sprostowania, usunięcia i ograniczenia przetwarzania danych;

Niedopełnienie obowiązku wynikającego z prawa do przenoszenia danych.

*Zgodnie z Dyrektywą 2000/31/WE Parlamentu Europejskiego i Rady w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, usługa społeczeństwa informacyjnego to usługa świadczona na odległość, drogą elektroniczną, za wynagrodzeniem i na indywidualne żądanie odbiorcy usługi.

8. ORGANY NADZORCZE

Ponieważ aktywność coraz większej liczby przedsiębiorców i organizacji wykracza poza granice jednego państwa, jednym z celów unijnej reformy przepisów o ochronie danych osobowych było wprowadzenie dla nich ułatwień. Chodzi tu przede wszystkim o jednolite przepisy oraz o ustanowienie jednego organu nadzorczego, który odpowiada za nadzór nad przetwarzaniem danych przez daną organizację czy przedsiębiorstwo. Taki organ ma koordynować wszystkie postępowania, w które są zaangażowane organy nadzorcze z innych krajów.

W świetle dotychczas obowiązujących przepisów organy nadzorcze (np. GIODO) posiadały uprawnienia jedynie w stosunku do podmiotów przetwarzających dane osobowe na terytorium własnego państwa. Zgodnie z RODO, w przypadku transgranicznego przetwarzania danych osobowych, organ nadzorczy państwa, na terytorium którego znajduje się główna jednostka organizacyjna administratora, jest tzw. organem wiodącym. Oznacza to, że posiada uprawnienia również jeśli chodzi o procesy przetwarzania dokonywane przez jednostki administratora w innych państwach.

WWW.GIODO.GOV.PL

Wskazanie jednego wiodącego organu nadzorczego jest konieczne, jeśli:

przetwarzanie odbywa się w jednostkach organizacyjnych danego przedsiębiorstwa czy organizacji w więcej niż jednym kraju (np. w przypadku operacji dokonywanych w międzynarodowych oddziałach danej spółki)

dany rodzaj przetwarzania znacznie wpływa na obywateli w więcej niż jednym kraju członkowskim (np. kiedy administrator z innego państwa nie ma w Polsce oddziału lub spółki zależnej, ale oferuje tu swoje usługi).

Organem wiodącym jest organ nadzorczy głównej jednostki organizacyjnej danego administratora - centralnej administracji. Centralna administracja w UE to miejsce, w którym zapadają decyzje co do celów i sposobów przetwarzania danych osobowych.

Więcej przydatnych informacji na ten temat znajdziesz w Wytycznych WP 244 Grupy Roboczej Art. 29, które dostępne są na stronie internetowej GIODO w zakładce „Reforma przepisów - Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244).

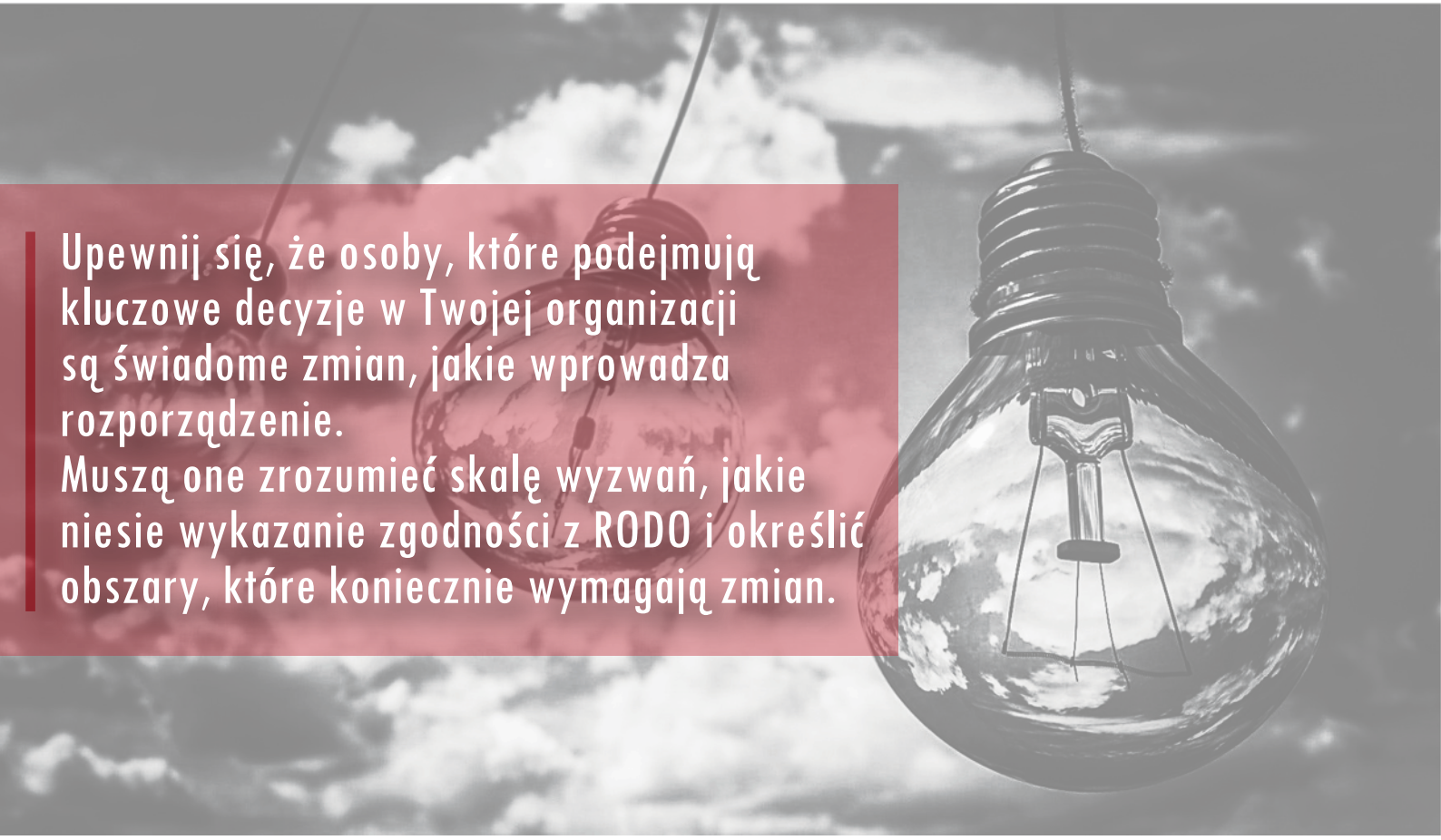
.

9. WIEDZA NA TEMAT RODO W ORGANIZACJI

Wobec skali zmian, jakie przynosi ogólne rozporządzenie o ochronie danych, przygotowanie się do jego stosowania jest dużym wyzwaniem. Zarówno dla dużych organizacji, w których w ten proces należy zaangażować wiele osób, jak i dla małych i średnich. Trzeba pracować przede wszystkim nad niezbędną wiedzą na temat nowych wymogów prawnych w zakresie przetwarzania danych osobowych.

Wszystkie osoby w organizacji i osoby blisko z nią współpracujące, które w jakikolwiek sposób uczestniczą w procesach przetwarzania danych, powinny mieć solidną wiedzę na temat nowych wymogów dotyczących bezpieczeństwa przetwarzania danych i praw osób fizycznych. Dzięki temu będą przygotowane do stosowania nowego prawa. Pomocnym rozwiązaniem może być udział w szkoleniach czy współpraca z profesjonalnymi firmami w celu wdrożenia rozporządzenia.

Najważniejsze, by dokonać rzetelnego przeglądu wszystkich prowadzonych czynności przetwarzania danych! Pomocne w tym zakresie będą wytyczne przygotowywane przez GIODO i Grupę Roboczą Art. 29.



Upewnij się, że osoby, które podejmują kluczowe decyzje w Twojej organizacji są świadome zmian, jakie wprowadza rozporządzenie.
Muszą one zrozumieć skalę wyzwań, jakie niesie wykazanie zgodności z RODO i określić obszary, które koniecznie wymagają zmian.

Powodzenia!

10. SPRAWDŹ SWOJĄ GOTOWOŚĆ NA RODO

Reforma przepisów o ochronie danych osobowych

- [ ] Czy wiesz, od kiedy RODO obowiązuje i jakie podstawowe zmiany wprowadza?

Nowe podejście do ochrony danych osobowych

- [ ] Czy słyszałeś o zasadzie rozliczalności i wiesz, jak wykazać zgodność z przepisami RODO?
- [ ] Czy wiesz, co oznacza podejście oparte na ryzyku?
- [ ] Czy wiesz, jak przeprowadzić ocenę ryzyka?

Zakres przetwarzanych informacji

- [ ] Czy zrobiłeś przegląd operacji przetwarzania danych w swojej organizacji?
- [ ] Czy wiesz jakie dane przetwarzacie?
- [ ] Czy wiesz na jakiej podstawie prawnej przetwarzane są te dane?

Nowe obowiązki informacyjne

- [ ] Czy wiesz, jakie zmiany nastąpią w odniesieniu do obowiązku informacyjnego?
- [ ] Czy wiesz, jak zmienić klauzulę informacyjną?

Uprawnienia osób fizycznych

- [ ] Czy znasz prawa osób, których dane dotyczą?
- [ ] Czy jesteś gotowy na realizację wniosków z ich strony dotyczących np. przeniesienia danych czy prawa do bycia zapomnianym?

Zgoda na przetwarzanie danych

- [ ] Czy pozyskiwane przez Ciebie zgody na przetwarzanie danych osobowych są dostosowane do wymogów rozporządzenia?

Zabezpieczenia

- [ ] Czy zdecydowałeś, jakie środki techniczne i organizacyjne zastosujesz, by zapewnić bezpieczeństwo danych osobowych i zgodność z przepisami RODO?

Dokumentacja przetwarzania danych

- [ ] Czy jesteś gotów do wewnętrznej rejestracji czynności przetwarzania danych?
- [ ] Czy masz odpowiednią dokumentację, aby wykazać zgodność z przepisami?

Ochrona danych w fazie projektowania i domyślna ochrona danych

- [ ] Czy znasz koncepcję ochrony danych w fazie projektowania oraz domyślnej ochrony danych?
- [ ] Czy uwzględniłeś je w swoich działaniach?

Ocena skutków dla ochrony danych

- [ ] Czy sprawdziłeś, czy jesteś zobowiązany do dokonania oceny skutków w zakresie ochrony danych?
- [ ] Czy wiesz, jak ją przeprowadzić?

Dane osobowe dzieci

- [ ] Czy oferując usługi skierowane do dzieci, przetwarzasz dane osobowe dzieci?
- [ ] Czy wiesz, jak pozyskiwać zgodę na przetwarzanie ich danych osobowych?

Automatyczne przetwarzanie danych oparte na profilowaniu

- [ ] Czy dokonujesz profilowania osób?
- [ ] Jeśli tak, to czy wiesz, jakie warunki musisz spełnić, aby działanie to było legalne?

Naruszenia ochrony danych

- [ ] Czy jesteś gotowy do wykrycia, analizy i zgłoszenia naruszenia ochrony danych?
- [ ] Czy wiesz, jakie działania musisz podjąć w przypadku wystąpienia takiego incydentu?

Inspektor ochrony danych (wcześniej ABI)

- [ ] Czy sprawdziłeś, czy jesteś zobowiązany do wyznaczenia inspektora ochrony danych?

Transgraniczne przetwarzanie danych

- [ ] Jeśli Twoja organizacja prowadzi działalność lub współpracuje w skali międzynarodowej, to czy wiesz, który organ będzie Twoim organem wiodącym?

Powierzenie danych

- [ ] Czy dokonałeś analizy dotychczasowych umów powierzenia, tak by firmy przetwarzające spełniały wszystkie wymagania wynikające z rozporządzenia?

Wiedzy na temat RODO w Twojej organizacji

- [ ] Czy osoby w Twojej organizacji, które mają dostęp do danych osobowych wiedzą o nowym rozporządzeniu i jego wymogach?
- [ ] Czy zaplanowałeś przeszkolenie tych osób?

ZAŁĄCZNIK NR 1

Kryteria dopuszczalnej oceny skutków dla ochrony danych

Kryteria, z których administratorzy danych mogą korzystać, aby ocenić, czy ocena skutków dla ochrony danych lub metodyka służąca do dokonania oceny skutków dla ochrony danych są wystarczająco kompleksowe do zachowania zgodności z RODO:

- ☐ zapewniono systematyczny opis operacji przetwarzania:
  - uwzględniono charakter, zakres, kontekst i cele przetwarzania;
  - w rejestrze zamieszczono dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych;
  - przedstawiono funkcjonalny opis operacji przetwarzania;
  - zidentyfikowano zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań);
  - uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania;
- ☐ oceniono niezbędność oraz proporcjonalność:
  - wskazano środki, których podjęcie jest planowane w celu zapewnienia przestrzegania rozporządzenia, uwzględniając:
    - środki przyczyniające się do proporcjonalności i niezbędności przetwarzania, z uwzględnieniem następujących aspektów:
      - konkretne, wyraźne i prawnie uzasadnione cele; zgodność przetwarzania z prawem;
      - dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
      - ograniczony czas przechowywania;
    - środki przyczyniające się do zachowania praw osób, których dane dotyczą:
      - poinformowanie osoby, której dane dotyczą;
      - prawo dostępu i prawo do przenoszenia danych;
      - prawo do sprostowania i do usunięcia danych;
      - prawo do sprzeciwu i prawo do ograniczenia przetwarzania;
      - relacje z podmiotem przetwarzającym;
      - zabezpieczenia przy międzynarodowym przekazywaniu danych;
      - uprzednie konsultacje;
- ☐ przeprowadzono działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą:
  - uwzględniono źródło, charakter, specyfikę i powagę ryzyka, czy konkretniej, w przypadku każdego rodzaju ryzyka (bezprawnego dostępu, niepożądanej zmiany i zniknięcia danych), z punktu widzenia osób, których dane dotyczą:
    - uwzględniono źródła ryzyka;
    - zidentyfikowano możliwe skutki dla praw i wolności osób, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych;
    - zidentyfikowano zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych;
    - oszacowano prawdopodobieństwo i powagę;
  - określono środki, których podjęcie jest planowane w celu zaradzenia ryzyku;
  - zaangażowano zainteresowane strony:
    - skonsultowano się z inspektorem ochrony danych w celu uzyskania zalecenia;
    - w stosownych przypadkach zasięgnięto opinii osób, których dane dotyczą, lub ich przedstawicieli.

ŹRÓDŁA

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych osobowych- RODO);
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2016.922);
- Data Protection Reform Factsheet http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404;
- Questions and Answers- Data protection reform http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm;
- EU Data Protection Reform: better rules for European businesses https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en;
- Better Data Protection rights for European citizens https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en;
- What is personal data? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en;
- What constitutes data processing? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en;
- It's your data – take control. https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf;
- The GDPR: new opportunities, new obligations https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf;
- Agreement on Commission's EU data protection reform will boost Digital Single Market http://europa.eu/rapid/press-release_IP-15-6321_en.htm;
- Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679 (WP260);
- Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 (WP248 rev.01);
- Proponowany wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych, opracowany przez GIODO https://giodo.gov.pl/pl/1520281/10430;
- Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO, opracowany przez GIODO https://giodo.gov.pl/pl/1520281/10449;
- Wytyczne dotyczące inspektorów ochrony danych ('DPO') (WP243 rew.01);
- Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244 rew.01);
- Czy jesteś gotowy na RODO? Opracowanie GIODO https://www.giodo.gov.pl/pl/1520281/10255;
- Jak rozumieć podejście oparte na ryzyku według RODO? Opracowanie GIODO https://giodo.gov.pl/pl/1520282/10294;
- Jak stosować podejście oparte na ryzyku? Opracowanie GIODO https://giodo.gov.pl/pl/1520282/10294;
- Building consumer trust, Protecting personal data in the consumer product industry; Consumer responses from the consumer product consumer and executive survey on data privacy and security, https://www2.deloitte.com/content/dam/insights/us/articles/consumer-data-privacy-strategies/DUP_970-Building-consumer-trust_MASTER.pdf;
- Zdjęcia wykorzystane w broszurze pochodzą z serwisu Pexels.com (licencja CC0). Dziękujemy autorom (imię i nazwisko/nazwa i nr strony, na której zamieszczono zdjęcie):Steven Arenas (2), Spencer Selover (3), rawpixel.com (4), Lucas (5), Sindre Strom (7), Sabrina Gelbart (8), Stefan Stefancik (9), Khaled Reese (10), Pixabay (6,11,12,14,17,19,20,23,24,26,27,28,31,33,34,36), Mike Chai (15), Gratisography (13), Stockpick (16), George Becker (30).