PRAWNE PODSTAWY DZIAŁALNOŚCI GOSPODARCZEJ
WYKŁAD III

Halszka Suszek-Borowska

RODO
PODSTAWA PRAWNA

Od wielu lat dane osobowe podlegają ochronie prawnej

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady

z dnia 24 października 1995r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych

Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych

(Dz. U. z 2014 r. poz. 1182, z późń. zm.)

Może regulacje i ograniczenia tej sfery życia wcale nie są potrzebne?

Rozporządzenie Parlamentu Europejskiego i Rady (UE)

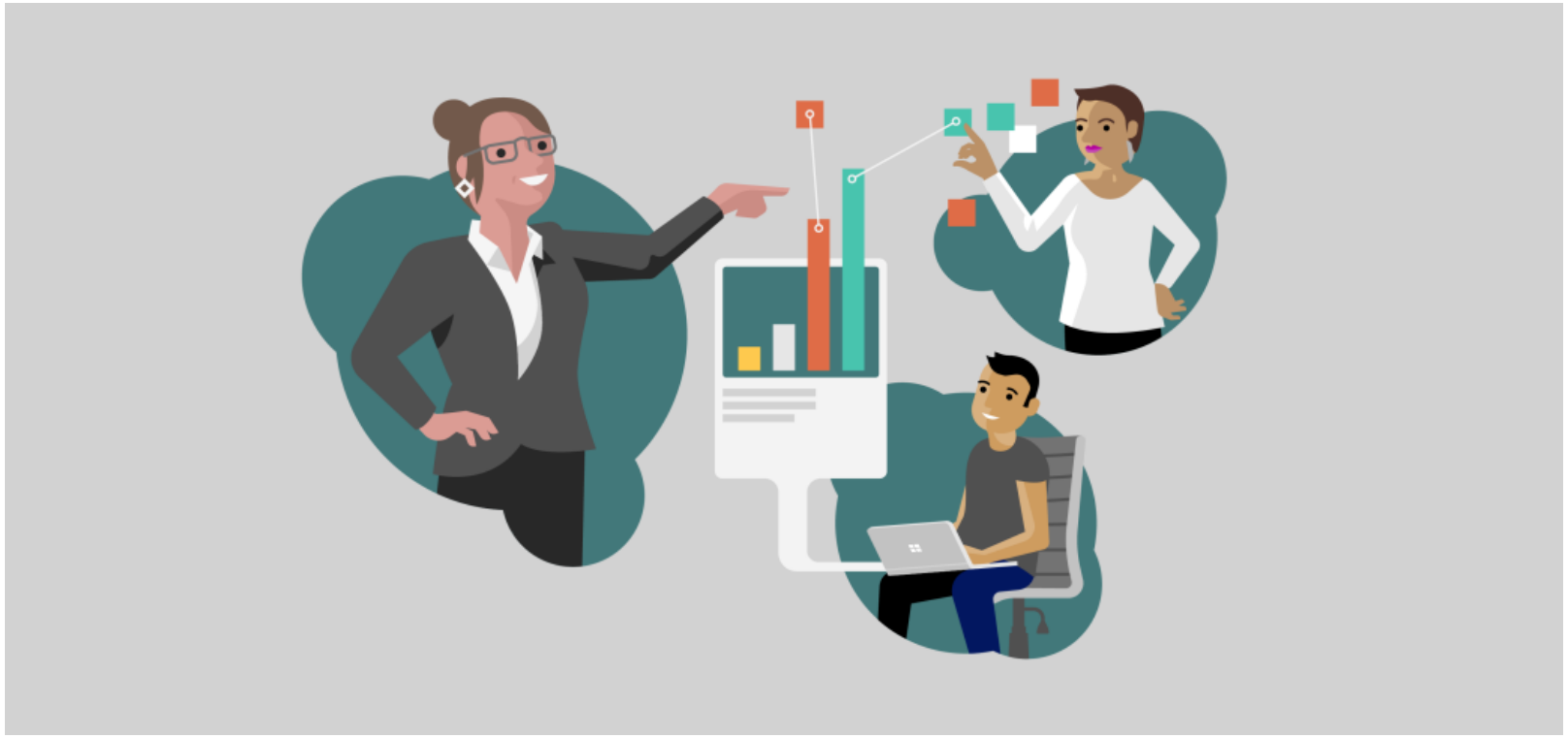
2016/679 z dn. 27 kwietnia 2016 roku

Ustawa o Ochronie Danych Osobowych

z 10 maja 2018r. **Dz.U. 2018 poz. 1000**

Wraz ze wzrostem wartości danych osobowych i rozwojem nowych technologii **konieczny jest wzrost wymogów prawnych związanych z ochroną tych danych.** Inaczej procedery, które traktujemy obecnie w kategoriach wyjątkowych, wycieki nielegalne wykorzystywanie danych osobowych – byłyby codziennością.

Nie ma wątpliwości, że ten standard powinien być coraz wyższy, proporcjonalny do zainteresowania danymi osobowymi.



DANE OSOBOWE

To informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej czyli osobie, której dane dotyczą, dodatkowo rozporządzenie wyjaśnia, że możliwa do zidentyfikowania osoba, to osoba którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie danych takich jak

- ✓ IMIĘ I NAZWISKO,
- ✓ NUMER IDENTYFIKACYJNY,
- ✓ DANE O LOKALIZACJI,
- ✓ IDENTYFIKATOR INTERNETOWY,
- ✓ JEDEN BĄDŹ KILKA SZCZEGÓLNYCH CZYNNIKÓW OKREŚLAJĄCYCH FIZYCZNĄ, FIZJOLOGICZNĄ, GENETYCZNĄ, PSYCHICZNĄ, EKONOMICZNĄ, KULTUROWĄ LUB SPOŁECZNĄ TOŻSAMOŚĆ OSOBY

Jakie są główne zmiany związane z wejściem RODO?

Prywatność

Osoby fizyczne mają prawo do:

- Dostępu do swoich danych
- Poprawy swoich danych
- Usunięcia danych
- Wstrzymania przetwarzania danych
- Przeniesienia swoich danych

Kontrole i powiadomienia

Organizacje powinny:

- Odpowiednio chronić dane
- Zgłaszać naruszenia danych
- Uzyskać odpowiednie zgody na przetwarzanie danych
- Utrzymywać szczegółową informację o przetwarzaniu danych

Przejrzyste zasady

Organizacje są zobowiązane:

- Transparentnie informować o zbieraniu danych
- Wskazać cel i zakres przetwarzania
- Określić czas przetwarzania danych oraz zasady ich usuwania

Technologia i szkolenia

Organizacje powinny:

- Przeszkolić pracowników
- Sprawdzać i odpowiednio zmieniać polityki przetwarzania danych
- Zatrudnić Inspektora Ochrony Danych (jeśli wymagane)
- Zmieniać i zarządzać kontraktami z dostawcami

Jak zacząć?

1. **Inwentaryzacja danych** – Zdefiniuj, jakie dane osobowe masz i gdzie one się znajdują
2. **Zarządzanie** – Zarządź, jak dane osobowe będą/są używane i kto może mieć do nich dostęp
3. **Ochrona** – Ustanów formy zabezpieczania do zapobiegania i wykrywania naruszeń, odpowiadania na wykryte podatności
4. **Raportowanie** – Twórz dokumentację – w szczególności na temat tego, kto ma dostęp do danych i procesów po wykryciu naruszenia

KILKA KLUCZOWYCH POJĘĆ

ADMINISTRATOR DANYCH

ADMINISTRATOR DANYCH to taki podmiot, który **decyduje o celach i sposobach przetwarzania danych. Innymi słowy, decyduje o tym, po co (cele) i jak (sposoby) wykorzystać dane osobowe.**

Przykłady!!!
- pracodawca w stosunku do danych osobowych swoich pracowników,
- sprzedawca w sklepie internetowym w stosunku do danych osobowych swoich klientów,
- właściciel strony internetowej w stosunku do danych osobowych osób, które zaprenumerowały newsletter.

Administratorem danych jest **zawsze określony podmiot** – np. spółka, a nie jej pracownik.

Przykłady!!!
- administratorem danych jest spółka z o.o., a nie jej prezes zarządu, czy dyrektor marketingu,
- administratorem danych jest Jan Kowalski prowadzący jednoosobową działalność gospodarczą.

ROZDZIAŁ IV

Administrator i podmiot przetwarzający

Sekcja 1

Obowiązki ogólne

Artykuł 24

Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

PODMIOT PRZETWARZAJĄCY

PODMIOT PRZETWARZAJĄCY dane osobowe **nie decyduje o celach i środkach przetwarzania danych** – działa na podstawie umowy z administratorem danych. Administrator danych może bowiem albo sam przetwarzać dane, albo skorzystać z usług zewnętrznego podmiotu, który te dane będzie przetwarzał dla niego.

Przykłady!!!

- biuro rachunkowe przetwarza na zlecenie dane osobowe przekazane mu w tym celu przez klientów,
- podmiot utrzymujący na zlecenie swoich klientów konta poczty elektronicznej przetwarza na zlecenie dane osobowe,
- podmiot zajmujący się profesjonalnie niszczeniem danych osobowych przetwarza w tym zakresie dane osobowe na zlecenie swoich klientów.

INSPEKTOR OCHRONY DANYCH (IOD)

Inspektor Ochrony Danych (IOD) to następca Administratora Bezpieczeństwa Informacji (ABI). Inaczej niż w przypadku ABI, wyznaczenie IOD w pewnych przypadkach jest obowiązkowe na gruncie RODO:

KIEDY?

- ✓ gdy dane są przetwarzane przez podmioty z sektora publicznego,
- ✓ 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, których dane dotyczą, na **dużą skalę,**
- ✓ gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących.

Sekcja 4

Inspektor ochrony danych

Artykuł 37

Wyznaczenie inspektora ochrony danych

1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) 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, których dane dotyczą, na dużą skalę; lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

2. Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

3. Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych.

INSPEKTOR OCHRONY DANYCH (IOD)

Nie każdy podmiot, którego główną działalnością jest przetwarzanie danych, musi jednak powołać IOD – a **tylko taki, którego działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę.**

Przykład!!!

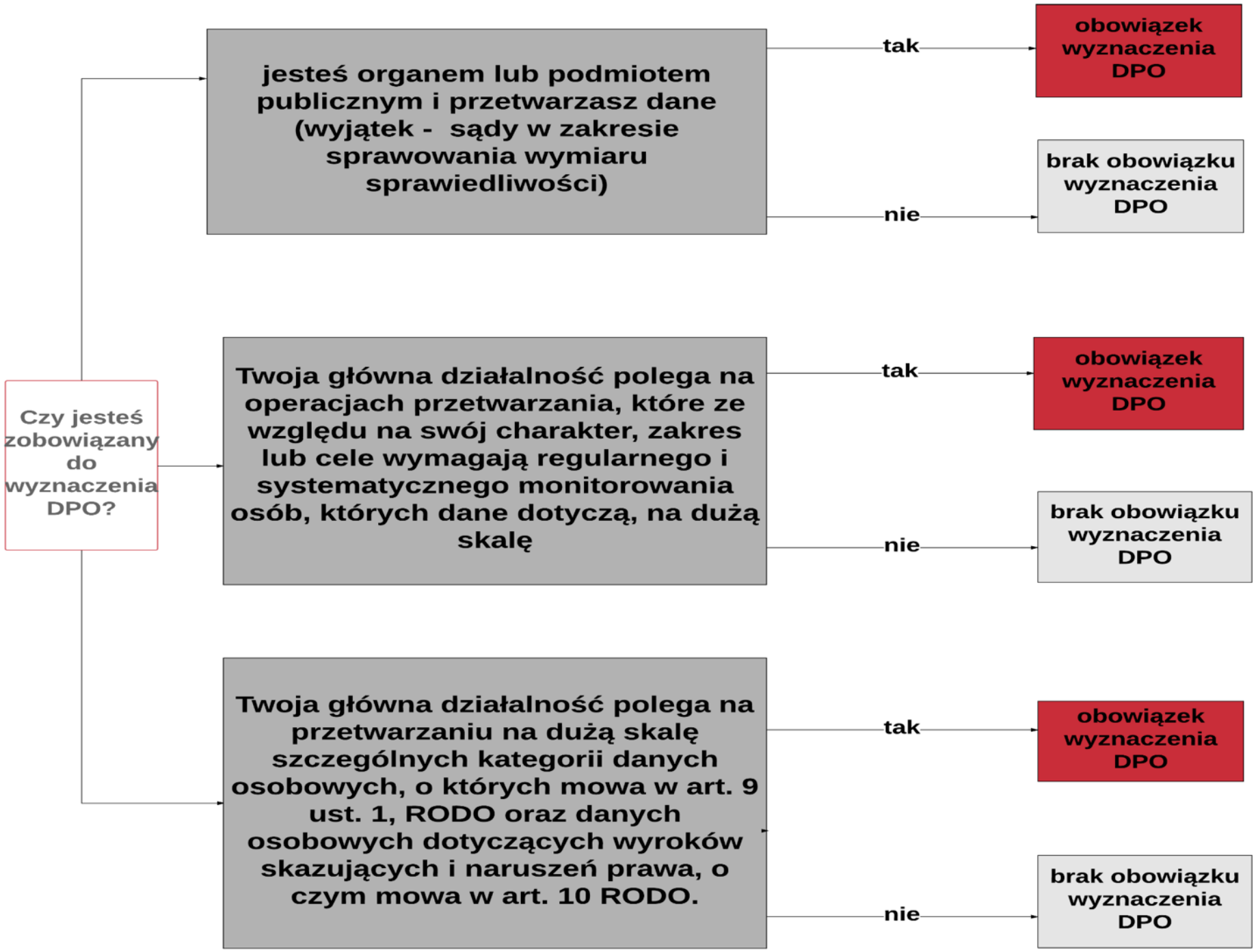
- Działalnością główną podmiotu zajmującego się profesjonalnym niszczeniem danych osobowych jest przetwarzanie danych osobowych, jednak podmiot ten nie ma obowiązku powołania IOD, ponieważ ta działalność nie wymaga regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę.

- Szpital powinien powołać IOD, choć jego główną działalnością jest leczenie, a przetwarzanie danych działalnością nierozerwalnie związaną z taką działalnością główną.

KTO MOŻE, A KTO MUSI WYZNACZYĆ INSPEKTORA OCHRONY DANYCH

RODO w art. 37 ust 1przewiduje obowiązek wyznaczenia inspektora dla administratorów i podmiotów przetwarzających wówczas, gdy:

- ✓ przetwarzania dokonują **organ lub podmiot** publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
- ✓ **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**, których dane dotyczą na **dużą skalę**.
- ✓ **główna działalność** administratora lub podmiotu przetwarzającego polega na przetwarzaniu **na dużą skalę** szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz **danych osobowych dotyczących wyroków skazujących i naruszeń prawa**, o których mowa w art. 10.



https://abi.giodo.gov.pl/inspektor-ochrony-danych/kto-moze-a-kto-musi-wyznaczyc-inspektora-ochrony-danych

PRAWA OSÓB KTÓRYCH DANE DOTYCZĄ

PRAWO DOSTĘPU DO DANYCH OSOBOWYCH

PODSTAWA PRAWNA: Art. 15 ust. 1

RODO wskazuje, że osoba, ktorej dane dotyczą, jest uprawniona do uzyskania od administratora (np. przedsiębiorcy) informacji, czy przetwarza on jej dane osobowe, a jeżeli ma to miejsce –
jest uprawniona do uzyskania dostępu do nich oraz do uzyskania informacji dotyczących:

- celów przetwarzania (np. cel marketingowy)
- kategorii danych które podlegają przetwarzan
- odbiorców lub kategorii odbiorców
- planowanego okresu przechowywania danych
- prawa do żądania sprostowania
- prawa wniesienia skargi do organu nadzorcze
- źródła dostarczającego dane osobowe
- zautomatyzowanego podejmowania decyzji

PRAWO DOSTĘPU DO DANYCH OSOBOWYCH

Prawo dostępu jest podstawowym i pryncypialnym prawem, a wszystkie pozostałe prawa wynikają właśnie z jego realizacji. Nieprawidłowe wypełnienie bądź niewypełnienie obowiązku w zakresie prawa dostępu do danych przez administratora (np. przedsiębiorcę), utrudni lub uniemożliwi wykonanie kolejnych praw. Dostęp do wymienionych wyżej kategorii informacji powinien zatem być skrupulatnie przestrzegany.

Przykład! *Działając w porozumieniu, wielu niezadowolonych klientow może kilka razy dziennie*
wnioskować o dostęp do ich danych, co albo całkowicie uniemożliwi normalne funkcjonowanie przedsiębiorstwa lub przynajmniej bardzo je zakłoci.

Aby ograniczyć nadużycia w tym zakresie, art. 15 ust. 3 RODO precyzuje, że **administrator** (np. przedsiębiorca) **jest zobowiązany do dostarczenia osobie, ktorej dane dotyczą, jednej nieodpłatnej kopii danych osobowych podlegających przetwarzaniu. Jednak za każdą kolejną administrator ma prawo pobrać opłatę w rozsądnej wysokości.** Wynika ona z kosztow administracyjnych związanych z dostarczeniem kopii danych
osobowych. Po uiszczeniu stosownej opłaty przez wnioskodawcę nie ma możliwości odmowienia mu dostępu

PRAWO DOSTĘPU DO DANYCH OSOBOWYCH
przykłady

Użytkowniczka jednego z portali społecznościowych wniosła do administratora o udostępnienie danych, ktore zostały na jej temat zebrane. W odpowiedzi dostała 1000 stron maszynopisu. Gdyby regularnie wnosiła o udostępnienie katalogu zebranych danych, mogłaby poważnie utrudnić funkcjonowanie portalu.

Prawo dostępu do danych dotyczy wszystkich podmiotow, czyli klientow, kontrahentow oraz pracownikow.

PRAWO DO SPROSTOWANIA DANYCH

PODSTAWA PRAWNA: Art. 16

Jedną z podstawowych zasad przetwarzania danych osobowych jest **zasada prawdziwości**. Wynika z niej **prawo do sprostowania danych, ktore przysługuje osobie zezwalającej na przetwarzanie jej danych.** Uwzględniając cel przetwarzania danych, osoba, ktorej dane dotyczą, ma **prawo żądania uzupełnienia i aktualizacji niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.** W takiej sytuacji aktualizacja czy uzupełnienie nastąpi bez usuwania dotychczasowych danych zgromadzonych tylko na mocy tego właśnie

Przedsiębiorca na stronie internetowej zamieszcza formularz dotyczący zmiany danych. Klienci mogą go wypełnić oraz przesyłać poprawione dane, gdyby zmienili adres zamieszkania, nazwisko itd.

PRAWO DO OGRANICZENIA PRZETWARZANIA

Osoba, ktorej dane dotyczą, korzystając z prawa dostępu, może nabrać przekonania, że np. **przetwarzanie odbywa się niezgodnie z prawem.** Powstaje więc sytuacja sporna – **administrator** (np. przedsiębiorca) **zbiera dane osobowe, a osoba zainteresowana uważa, że nie ma on ku temu podstaw**. Dlatego w rozporządzeniu przewidziano rownież **rozwiązanie zabezpieczające**, ktore zostało ujęte jako **przysługujące prawo**

PRAWO DO OGRANICZENIA PRZETWARZANIA

Uwaga!!!

W RODO nie zawarto definicji ograniczenia przetwarzania, a jedynie wskazano w nim przypadki, kiedy ono następuje. **Jest to prawo podobne do prawa do bycia zapomnianym, z tą rożnicą, że administrator, pomimo ograniczenia przetwarzania, może następnie przetwarzać te dane za zgodą osoby w sytuacjach określonych w**
art. 18 ust. 2 np.

- ✓ **ochrony własnych roszczeń**
- ✓ **proces sądowy o zniesławienie,**
- ✓ **naruszenie dobr osobistych**

Jest to zatem prawo, ktore będzie wykorzystywane przy okazji pozwów sądowych lub skarg do organu nadzorczego, gdy klient, pracownik lub kontrahent uważa, że administrator nie ma podstaw do przetwarzania lub przetwarzane dane nie są

PRAWO DO OGRANICZENIA PRZETWARZANIA przykład

PODSTAWA PRAWNA: Art. 18 ust. 1

RODO określa sytuacje, w których osoba, ktorej dane są przetwarzane, ma prawo żądać ograniczenia tej czynności.

KIEDY TAK SIĘ DZIEJE?

OSOBA, KTOREJ DANE DOTYCZĄ, KWESTIONUJE PRAWIDŁOWOŚĆ DANYCH OSOBOWYCH – NA OKRES POZWALAJĄCY ADMINISTRATOROWI SPRAWDZIĆ PRAWIDŁOWOŚĆ TYCH DANYCH;

Klient sklepu zmienił nazwisko, o czym właściciel sklepu został poinformowany. Jednak, łamiąc zasadę prawdziwości danych, administrator nie zmienił danych. Dopóki administrator nie sprawdzi, czy dane klienta odpowiadają prawdzie, nie może ich przetwarzać np. do celow marketingowych. Okres aktualizacji będzie zależał od samego przedsiębiorcy.

PRAWO DO BYCIA ZAPOMNIANYM

PRAWO TO SKŁADA SIĘ Z DWÓCH UPRAWNIEŃ:

- ✓ możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez administratora,

- ✓ możliwości żądania, aby administrator danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych lub ich kopie.

PRAWO DO BYCIA ZAPOMNIANYM

PRAWO DO BYCIA ZAPOMNIANYM MOŻNA WYKONAĆ, JEŻELI SPEŁNIONA JEST CHOĆ JEDNA Z NASTĘPUJĄCYCH PRZESŁANEK:

a) jeżeli **dane osobowe nie są już niezbędne do celów**, w których zostały zebrane lub w inny sposób przetwarzane,
b) jeżeli osoba, której dane dotyczą, **wycofała zgodę na przetwarzanie danych osobowych** i nie istnieje inna podstawa przetwarzania danych,
c) jeżeli osoba, której dane dotyczą, **zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych,**
d) jeżeli dane osobowe **były przetwarzane „niezgodnie z prawem”,**
e) jeżeli dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator”,
f) jeżeli dane osobowe **zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.**

PRAWO DO BYCIA ZAPOMNIANYM

Administrator danych osobowych przetwarza na podstawie zgody dane osobowe w celu marketingowym. Osoba, której dane dotyczą, wycofuje zgodę oraz korzysta z prawa do bycia zapomnianym.

W przypadku wykonania prawa do bycia zapomnianym, **administrator danych powinien zaprzestać przetwarzania danych osobowych i usunąć dane, chyba że zachodzą szczególne przypadki ograniczające prawo do bycia zapomnianym.**

a) istnienie przepisu prawa, który nakazuje przetwarzanie danych osobowych,
b) sytuacja, w której przetwarzanie danych jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

PRZYKŁAD!!

Klient sklepu internetowego zamówił książkę, którą otrzymał, ale za którą nie zapłacił. Następnie postanawia wykonać prawo do bycia zapomnianym – administrator danych może jednak jego dane nadal przetwarzać, ponieważ jest mu to niezbędne do dochodzenia swoich praw przed sądem.

PRZYKŁAD!!!
Klient sklepu internetowego zamówił książkę, za którą zapłacił i otrzymał fakturę. Następnie postanawia wykonać prawo do bycia zapomnianym – administrator danych może jednak jego dane nadal przetwarzać, ponieważ obowiązek przetwarzania danych wynika z przepisów o rachunkowości.

W przypadku wykonania prawa do bycia zapomnianym, **administrator danych powinien także poinformować innych administratorów danych, którym upublicznił dane osobowe**, że osoba, której dane dotyczą, żąda, **by administratorzy ci usunęli wszelkie łącza do tych danych oraz kopie tych danych osobowych.**

Obowiązek ten może być ograniczony przez:
a) dostępną technologię,
b) koszty,
c) konieczność ograniczenia do „rozsądnych działań”

Ograniczenie zakresu obowiązku przy użyciu kryterium kosztów powoduje, że podmioty większe, o większych możliwościach finansowych, będą zobowiązane do wykonywania tego obowiązku w szerszym zakresie niż podmioty niewielkie, mające mniejsze dostępne zasoby finansowe. Z kolei poprzez przywołanie „rozsądnych działań” ograniczono charakter obowiązku w ten sposób, że nie ma on charakteru zobowiązania rezultatu, a wyłącznie starannego działania.

PRAWO DO PRZENOSZENIA DANYCH

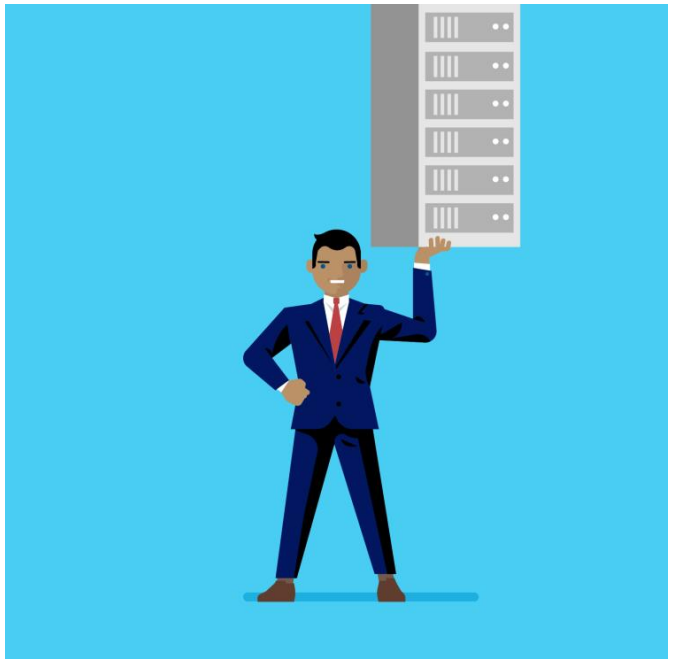
TO PRAWO DO:

- ✓ **otrzymania przez osobę**, której dane dotyczą, ustrukturyzowanego, powszechnie używanego formatu (np. PDF), który będzie nadawał do odczytu maszynowego, z **danymi osobowymi które dostarczyła administratorowi,**

- ✓ **żądania by dotychczasowy administrator danych przesłał dane osoby której one dotyczą, innemu podmiotowi.**

PRAWO DO PRZENOSZENIA DANYCH

PODSTAWA PRAWNA: art. 20 RODO



Prawo do przenoszenia danych może być wykonane wyłącznie wtedy, gdy:

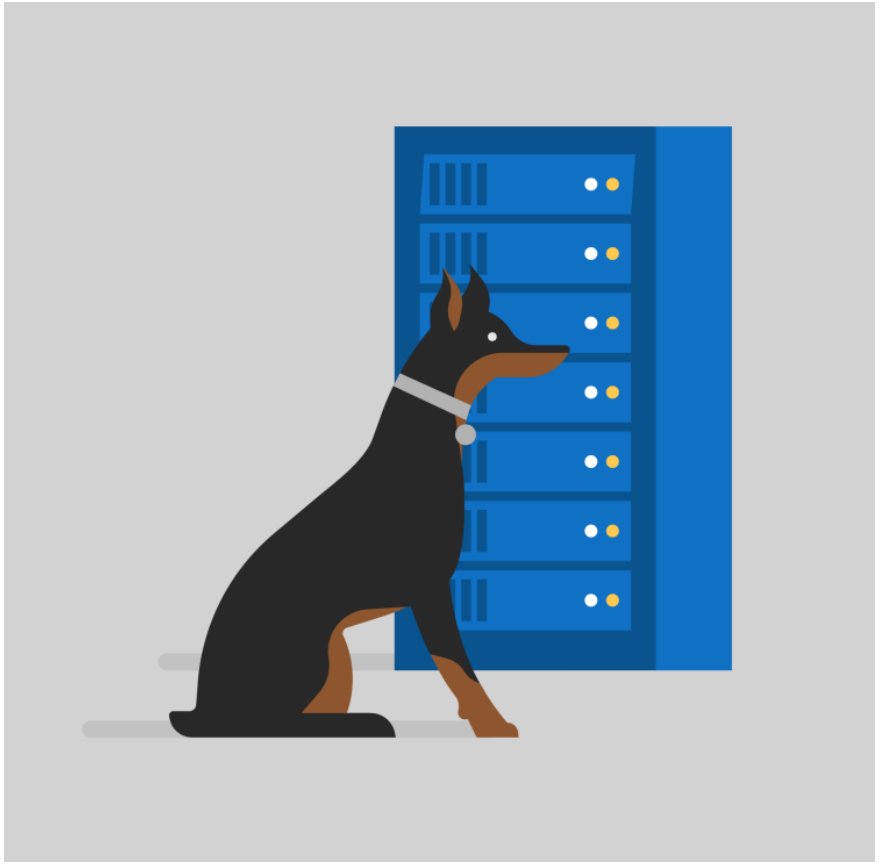
- ✓ przetwarzanie danych odbywa się na podstawie zgody lub w celu wykonania umowy
- ✓ przetwarzanie danych odbywa się w sposób zautomatyzowany.

Prawo do przenoszenia danych **obejmuje tylko dane osobowe przetwarzane przy użyciu systemów informatycznych i nie obejmuje tradycyjnych, papierowych zbiorów danych.**
Prawo do przenoszenia danych **obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo i które to dane ta osoba dostarczyła administratorowi.**

OBOWIĄZEK INFORMACYJNY

CO TO JEST OBOWIĄZEK ZGŁASZANIA NARUSZEŃ OCHRONY DANYCH?

RODO nakłada na podmioty przetwarzające dane osobowe prawny obowiązek informowania o incydentach bezpieczeństwa dotyczących danych osobowych.



Incydent bezpieczeństwa zwany jest w przepisach RODO naruszeniem ochrony danych osobowych i może polegać na:

- ✓ naruszeniu bezpieczeństwa prowadzącym do **przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania danych osobowych**
- ✓ naruszeniu bezpieczeństwa prowadzącym do **nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych**.

OBOWIĄZEK INFORMACYJNY

PRZYKŁADY!!!

- ✓ zagubienie nośnika z danymi osobowymi,
- ✓ uzyskanie dostępu do danych przez osobę do tego nieuprawnioną,
- ✓ włamanie do systemu służącego do przetwarzania danych osobowych.

O wystąpieniu incydentu **należy poinformować organ nadzorczy** (PUODO). Informacja powinna zostać przekazania niezwłocznie, lecz nie później, niż **w ciągu 72 godzin od stwierdzenia naruszenia**. W pewnych przypadkach **należy również informować o incydencie osoby, których dane dotyczą** – będzie tak wtedy, gdy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą.

PODSTAWA PRAWNA: art. 34 RODO

JAK ZAWRZEĆ UMOWĘ POWIERZEINA PRZETWARZANIA DANYCH

PODSTAWA PRAWNA
Art. 28, 42 RODO

Umowa powierzenia może zostać zawarta w formie pisemnej oraz w formie elektronicznej, pod warunkiem zapewnienia integralności i autentyczności dokumentu w postaci elektronicznej.

JAK ZAWRZEĆ UMOWĘ POWIERZEINA PRZETWARZANIA DANYCH

W działalności większości przedsiębiorców dochodzi do powierzenia przetwarzania danych osobowych.

PRZYKŁADY!!!

- ✓ **korzystanie z usług zewnętrznego podmiotu świadczącego usługi księgowe,**
- ✓ korzystanie z usług podmiotu zapewniającego **usługi poczty elektronicznej,**
- ✓ zlecenie zewnętrznemu podmiotowi **zniszczenia dokumentów zawierających dane osobowe,**
- ✓ zlecenie zewnętrznemu podmiotowi **archiwizacji dokumentów zawierających dane osobowe.**

RODO WPROWADZA NOWE WYMAGANIA CO DO TREŚCI UMOWY POWIERZENIA

Są to zobowiązania podmiotu przetwarzającego do:

a) przetwarzania danych wyłącznie na udokumentowane polecenie administratora,
b) zapewniania, aby **osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy** lub by podlegały odpowiedniemu **ustawowemu obowiązkowi zachowania tajemnicy,**
c) podejmowania środków zabezpieczenia danych wymaganych przez RODO i pomagania administratorowi wywiązać się z tych obowiązków,
d) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego – tzw. podpowierzenie przetwarzania danych jest dopuszczalne wyłącznie za zgodą administratora danych,
e) pomagania administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, **w zakresie wykonywania jej praw określonych w RODO**,
f) usunięcia danych lub do zwrotu danych administratorowi danych po zakończeniu przetwarzania, zgodnie z decyzją administratora,
g) udostępnia administratorowi wszelkich informacji niezbędnych do wykazania spełnienia jego obowiązków oraz do **umożliwiania administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów.**

JAK ZAWRZEĆ UMOWĘ POWIERZEINA PRZETWARZANIA DANYCH

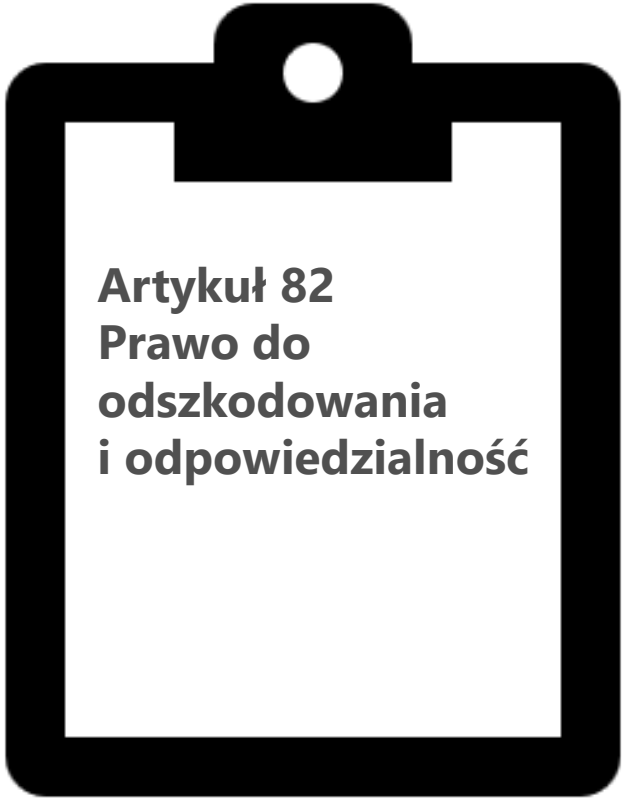
PODSTAWA PRAWNA
Art. 28, 42 RODO

Na Administrartorze ciąży **prawny obowiązek wyboru takiego podmiotu przetwarzającego, który gwarantuje odpowiednią ochronę danych osobowych**.

Administrator danych może mieć praktyczną trudność w wyborze takiego podmiotu – zwłaszcza, gdy sam jest podmiotem niewielkim, a przetwarzanie danych ma się odbywać przez renomowanych dostawców.

CO TERAZ?

Z pomocą przychodzi tzw. **procedura certyfikacji podmiotów przetwarzających dane osobowe.**
Certyfikaty wydawane będą po to, żeby **zaświadczyć o zgodności przetwarzania danych przez certyfikowany podmiot.** Będzie to więc wskazówka dla tych, którzy poszukują odpowiedniego podmiotu przetwarzającego dane osobowe – wybór podmiotów posiadających certyfikat



1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać **od administratora lub podmiotu przetwarzającego** odszkodowanie za poniesioną szkodę.

2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. **Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające**, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

(81) Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług **wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania.** (...)

Biorąc pod uwagę zapis art. 82 RODO, bardzo ważną kwestią jest powierzenie danych wiarygodnemu podmiotowi przetwarzającemu. Coraz więcej organizacji decyduje się na migrację do chmury. Zanim potencjalni klienci wykonają ten krok, powinni zadać dostawcy usług w chmurze kilka pytań dotyczących ochrony prywatności.. Dostawcy chmury dbają o jakość swoich usług. Dostosowanie ich do wymogów Rozporządzenia stało się priorytetem. Poniżej cztery podstawowe filary o których warto pamiętać.

ZABEZPIECZENIA

Moje dane są odpowiednio chronione – i technicznie i organizacyjnie

PRYWATNOŚĆ

Moje dane należą do mnie i to ja chcę je kontrolować

ZGODNOŚĆ

Chcę mieć pewność i gwarancje, że dostawca chmury stosuje te środki

JAWNOŚĆ

Chcę wiedzieć, gdzie i w jaki sposób dostawca przechowuje moje dane

Czy dane w chmurze są bezpieczne?

Wybierając operatora chmury, administrator danych powinien zwrócić szczególną uwagę na gwarancje ochrony danych operatora. Takimi gwarancjami są m.in. stosowanie zatwierdzonego branżowego kodeksu postępowania (art. 40 RODO) oraz stosowanie zatwierdzonego mechanizmu certyfikacji (art. 42. RODO).

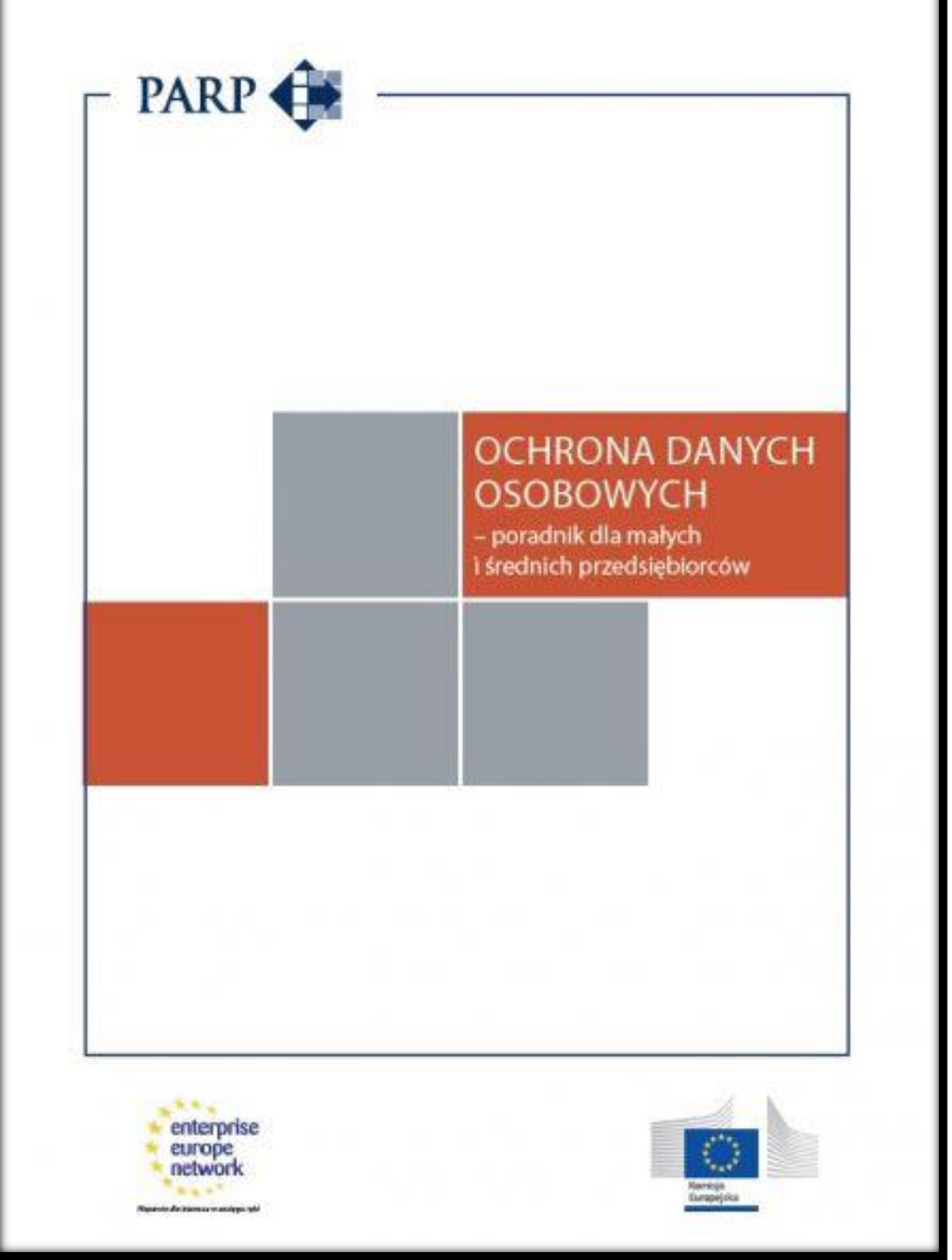
Dzięki certyfikacjom i znakom jakości oraz oznaczeniom w dziedzinie ochrony danych, użytkownicy chmury mają możliwość szybkiej oceny stopnia ochrony danych przy oferowanych i świadczonych usługach w ramach cloud computingu. Poddanie się przez operatora chmury weryfikacji przez organy kontrolne UE świadczy o jego wiarygodności i zaangażowaniu w kwestię ochrony danych osobowych.

Normy techniczne

Posiadanie przez operatorów certyfikatów norm technicznych powinno stanowić ważną wskazówkę dla administratora danych podczas procesu wyboru konkretnej chmury obliczeniowej. W Europie tworzenie norm oraz ich certyfikowanie zostało powierzone Europejskiemu Instytutowi Norm Telekomunikacyjnych (ETSI).

Najistotniejsze są dwa akty: norma ISO/IEC 27001 dotycząca zarządzania bezpieczeństwem informacji oraz norma ISO/IEC 27018 odnosząca się bezpośrednio do bezpieczeństwa danych osobowych w chmurze.

Jeżeli operator dostosował swoje działania do wyżej wskazanych norm technicznych, możemy uznać, że stosuje się on do tzw. kodeksu dobrych praktyk.



MATERIAŁY POMOCNICZE

Ponieważ temat dotyczący RODO cieszy się obecnie ogromnym zainteresowaniem, jeśli masz dodatkowe pytania, zapraszam do kontaktu. Na codzień zajmuję się ochroną danych osobowych więc może będę mogła pomóc dzieląc się doświadczeniem, materiałami, oraz informacjami dotyczącymi spotkań na temat RODO.

Ale na początek zacznij od poradnika który z pewnością rozwieje część Twoich wątpliwości i pomoże przygotować się do zaliczenia ;)

http://www.een.org.pl/index.php/publikacje-573/items/ochrona-danych-osobowych-poradnik-dla-malych-i-srednich-przedsiebiorcow.html

ODPOWIEDZIALNOŚĆ

- ✓ Za naruszenie ochronydanych odpowiadamy do €10M/2%
- ✓ Za niezapewnienie dostępu przy kontroli do €20M/4%
- ✓ Ciężar dowodu zgodności spoczywa na nas (5.2. RODO - rozliczalność)