



lubasz&wspólnicy

KANCELARIA RADCÓW PRAWNYCH

RODO. Wszystko co musi wiedzieć marketingowiec

Witold Chomiczewski

Zasięg terytorialny

RODO ma zastosowanie

- do przetwarzania danych osobowych w związku z działalnością prowadzoną przez administratora lub procesora w UE, niezależnie od tego, czy przetwarzanie odbywa się w UE,
- do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w UE przez administratora lub procesora niemających jednostek w UE – jeżeli czynności przetwarzania wiążą się z:
 - oferowaniem towarów lub usług takim osobom, których dane dotyczą, w UE – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
 - monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w UE.

Dane osobowe

wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej

osobą możliwą do zidentyfikowania jest taka, której tożsamość można określić bezpośrednio lub pośrednio

w szczególności na podstawie identyfikatora takiego jak: imię, nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy, lub co najmniej jedno znak szczególny związany z jej tożsamością



lubasz&wspólnicy

KANCELARIA RADCÓW PRAWNYCH

Przetwarzanie

Gromadzenie

Utrwalanie

Organizowanie

Porządkowanie

Przechowywanie

**Adaptowanie /
modyfikowanie**

Pobieranie

Przeglądanie

Wykorzystywanie

Ujawnianie

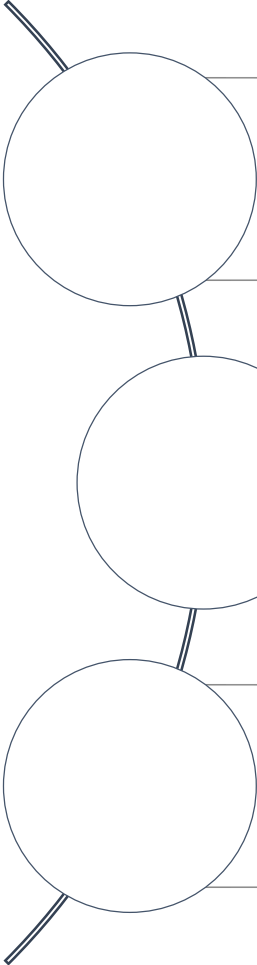
**Dopasowywanie /
łączenie**

**Rozpowszechniani
e**

Ograniczanie

**Usuwanie /
niszczenie**

Administrator



osoba fizyczna lub prawna,

organ publiczny, jednostka lub inny podmiot,

który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Współadministratorzy

Wspólnie ustalają cele i sposoby przetwarzania

Uzgodnienia zgodnie z faktyczną rolą każdego administratora

- Podział zadań w zakresie wypełnienia obowiązków z RODO
- Zasady korzystania przez podmiot danych z przysługujących mu praw
- Podział obowiązków informacyjnych

Uzgodnienia - udostępniane podmiotowi danych

Podmiot danych – prawo do korzystania z przysługujących mu praw

- W odniesieniu do każdego administratora
- Przeciwko każdemu administratorowi

Podmiot przetwarzający i odbiorca

podmiot przetwarzający

- Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

odbiorca

- Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.
- Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania, nie są jednak uznawane za odbiorców.

Powierzenie

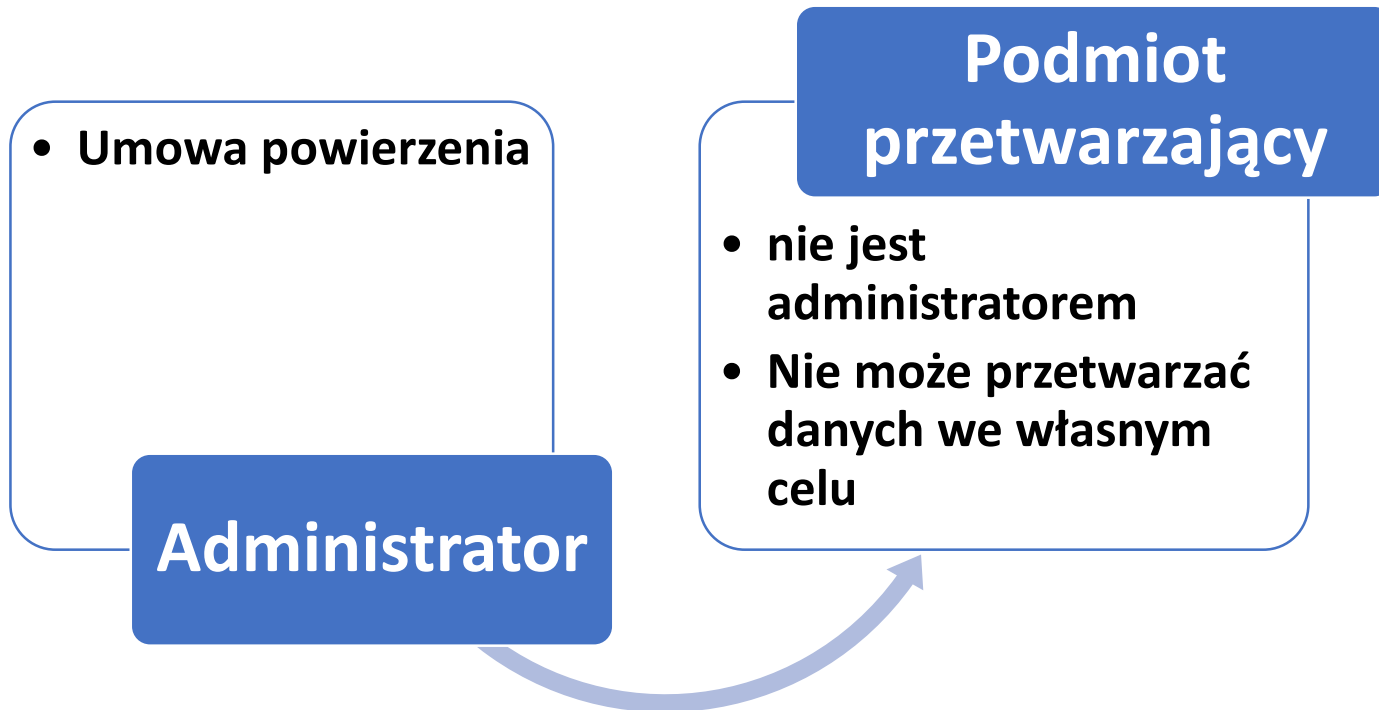
Wybór – wyłączna decyzja administratora

Odpowiedzialność za poprawność wyboru - administrator

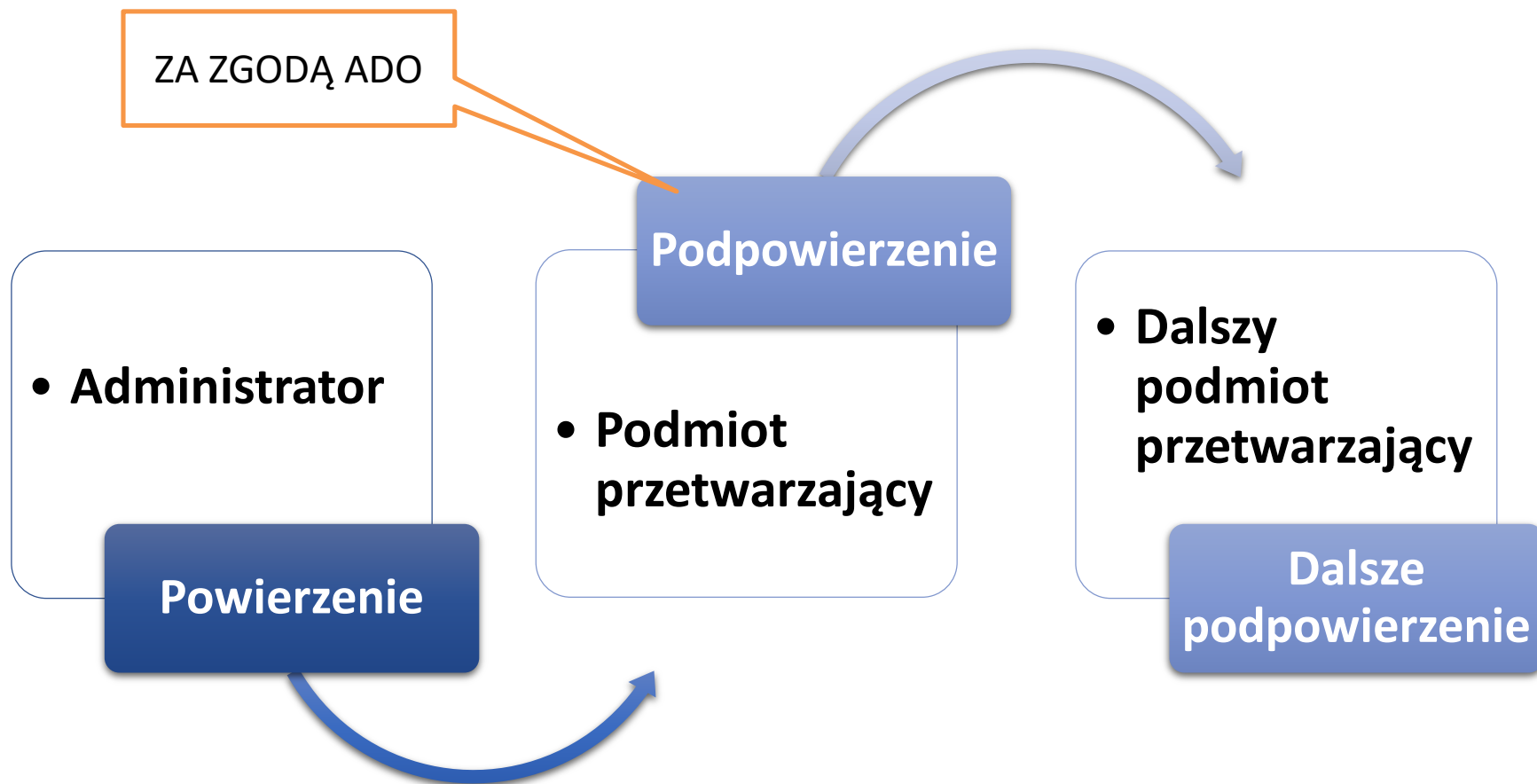
Możliwość korzystania z usług procesora

- O ile zapewnia on wystarczające gwarancje wdrożenia odpowiednich środków, by:
 - przetwarzanie spełniało wymogi RODO
 - chroniło prawa osób, których dane dotyczą

Relacja powierzenia



Możliwość dokonywania dalszych powierzeń



Zasady przetwarzania danych

Legalność

Rzetelność

Przejrzystość

Celowość

**Minimalizacja
danych**

Proporcjonalność

**Ograniczenie
czasowe**

Integralność

Poufność

Rozliczalność

Przesłanki przetwarzania

Zgoda

Wykonanie umowy

Niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze

Ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

Niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

Niezbędność do celów wynikających z uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią

Zgoda osoby, której dane dotyczą

Okazanie woli

- Dobrowolne
- Konkretnie
- Świadome
- Jednoznaczne

Forma

- Oświadczenie
- lub wyraźne działanie potwierdzające

Cel okazania woli

- przyzwolenie na przetwarzanie

Dodatkowe warunki - zgoda

ADO musi być w stanie wykazać, że udzielono zgody

Zgoda w pisemnym oświadczeniu

- Zapytanie o zgodę – wyraźnie oddzielone od innych kwestii
- Zapytanie w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem

Wycofanie zgody

- W każdym momencie
- Nie wpływa na zgodność z prawem przetwarzania przed wycofaniem zgody
- Musi być równie łatwe jak jej udzielenie

Zgoda dziecka

Zgoda udzielana przez dziecko w związku z usługami społeczeństwa informacyjnego – dotyczy:

- Usług oferowanych bezpośrednio dziecku
- Wiek: poniżej 16. roku życia

Nie wpływa na ogólne przepisy prawa umów dot. ważności, trybu zawierania i skutków umowy wobec dziecka

Zasada: wymóg udzielenia zgody przez osobę sprawującą władzę rodzicielską nad dzieckiem lub zaaprobowania zgody przez taką osobę

Obowiązek administratora

- Podjęcie racjonalnych starań, by zweryfikować, czy osoba sprawująca władzę rodzicielską udzieliła zgody

Prawnie uzasadniony interes

Prawnie uzasadniony interes administratora

Niezbędność przetwarzania dla realizacji celu

Podstawowe prawa i wolności podmiotu danych oraz jego interesy

Co jest nadrzędne?

- charakter interesu, rodzaj prawa lub wolności, sposób przetwarzania danych, zagrożenia z niego wynikające, relacje z administratorem, łatwość zatrzymania przetwarzania, liczba podmiotów przetwarzających dane

Dane szczególnych kategorii

Zasada

- Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby lub danych dotyczących zdrowia lub seksualności i orientacji seksualnej.

Wyjątki od ogólnego zakazu

Zgoda

Obowiązki i prawa
w dziedzinie prawa pracy,
zabezpieczenia społecznego
i ochrony społecznej

Ochrona żywotnych interesów

Działalność fundacji,
stowarzyszeń, podmiotów
niezarobkowych o celach
politycznych, związkowych,
religijnych

Dane podane w sposób
wyraźny do wiadomości
publicznej przez podmiot
danych

Ustalenie, dochodzenie,
obrona roszczeń

Interes publiczny w dziedzinie
zdrowia publicznego

Profilaktyka zdrowotna,
medyczny pracy, zarządzenia
systemami i usługami opieki
zdrowotnej lub społecznej

Cele archiwizacyjne, badania
naukowe, cele statystyczne

Prawa podmiotu danych

Zasada przejrzystości

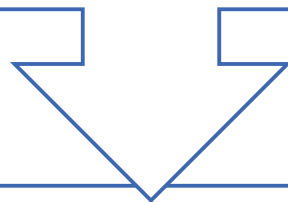
Administrator w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udziela osobie, której dane dotyczą, wszelkich informacji

- Informacji udziela się na piśmie lub innymi sposobami, a w stosownym przypadku – elektronicznie np. za pomocą strony internetowej
- Gdy komunikaty skierowane do dziecka – tak prosty i łatwy język by dziecko mogło zrozumieć

Administrator ułatwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw

Realizacja praw

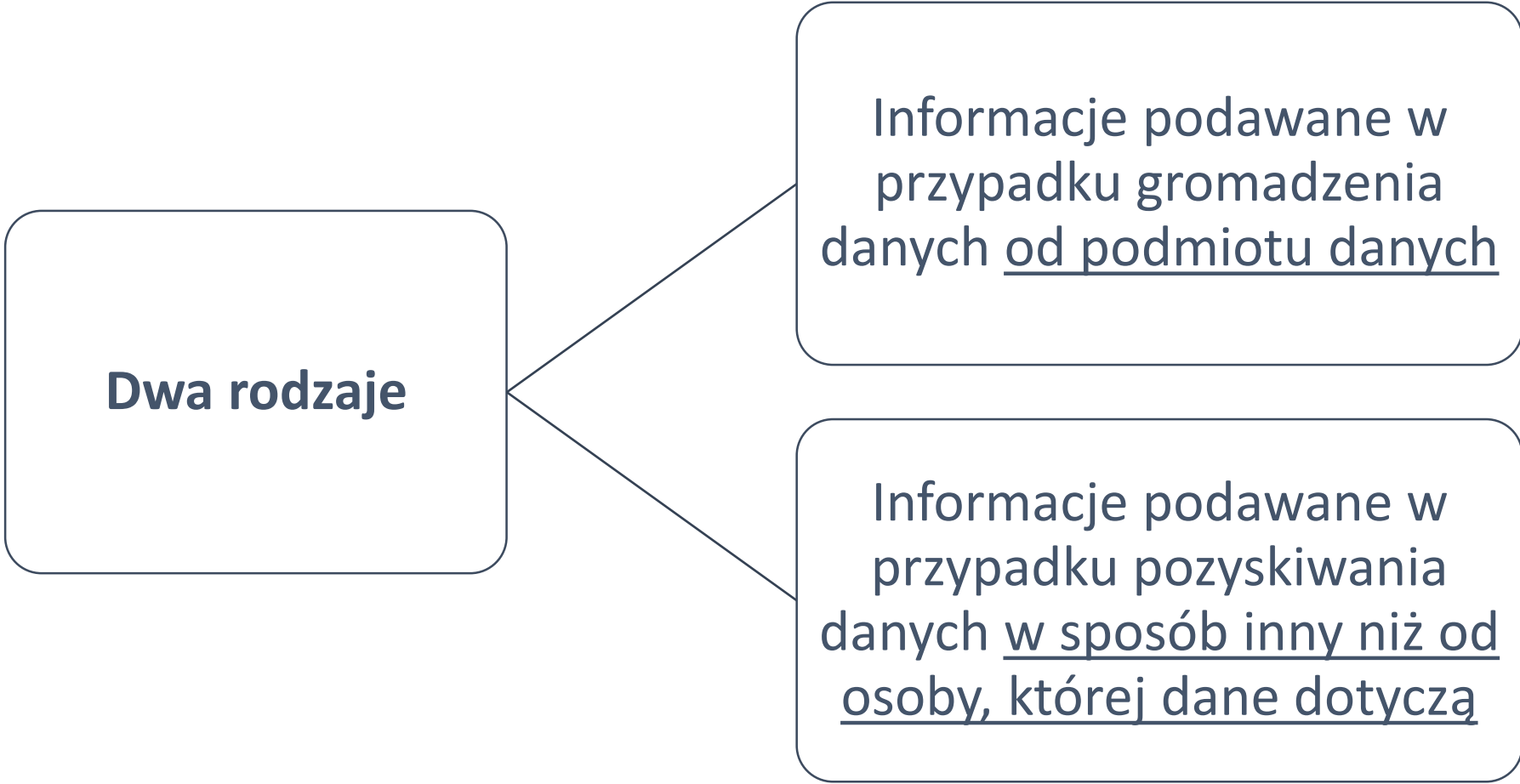
Administrator bez zbędnej zwłoki – najpóźniej w terminie miesiąca od otrzymania wniosku – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z wnioskiem.



Jeżeli administrator nie podejmuję/w działań to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania wniosku – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania z sądowych środków ochrony prawnej.

Obowiązek informacyjny

Dwa rodzaje



```
graph LR; A[Dwa rodzaje] --- B[Informacje podawane w przypadku gromadzenia danych od podmiotu danych]; A --- C[Informacje podawane w przypadku pozyskiwania danych w sposób inny niż od osoby, której dane dotyczą];
```

Informacje podawane w przypadku gromadzenia danych od podmiotu danych

Informacje podawane w przypadku pozyskiwania danych w sposób inny niż od osoby, której dane dotyczą



lubasz&wspólnicy

KANCELARIA RADCÓW PRAWNYCH

Obowiązek informacyjny – art. 13

Bezpośrednie zbieranie danych – podawane informacje:

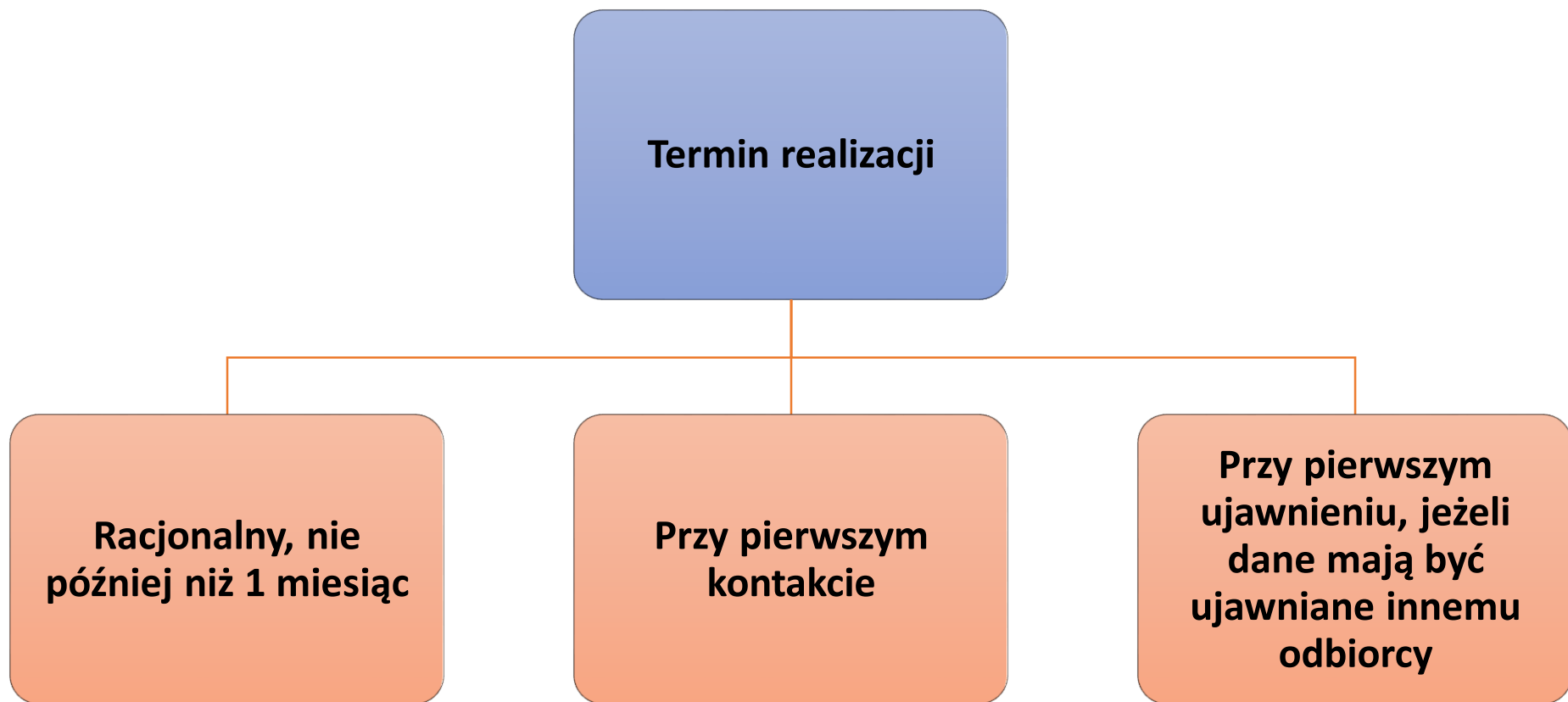
- tożsamość ADO i dane kontaktowe oraz dane kontaktowe inspektora ochrony danych
- cele przetwarzania danych osobowych oraz podstawa prawna
- uzasadnione interesy realizowane przez administratora lub przez stronę trzecią
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców
- informacje o przekazywaniu danych do państw trzecich
- okres przechowywania danych
- informacje o uprawnieniach podmiotu danych (w tym o cofnięciu zgody)
- prawo wniesienia skargi do organu nadzorczego
- dobrowolność lub obowiązek podania danych + konsekwencje ich niepodania
- informacje o zautomatyzowanym podejmowaniu decyzji
- planowana zmiana celu

Obowiązek informacyjny – art. 14

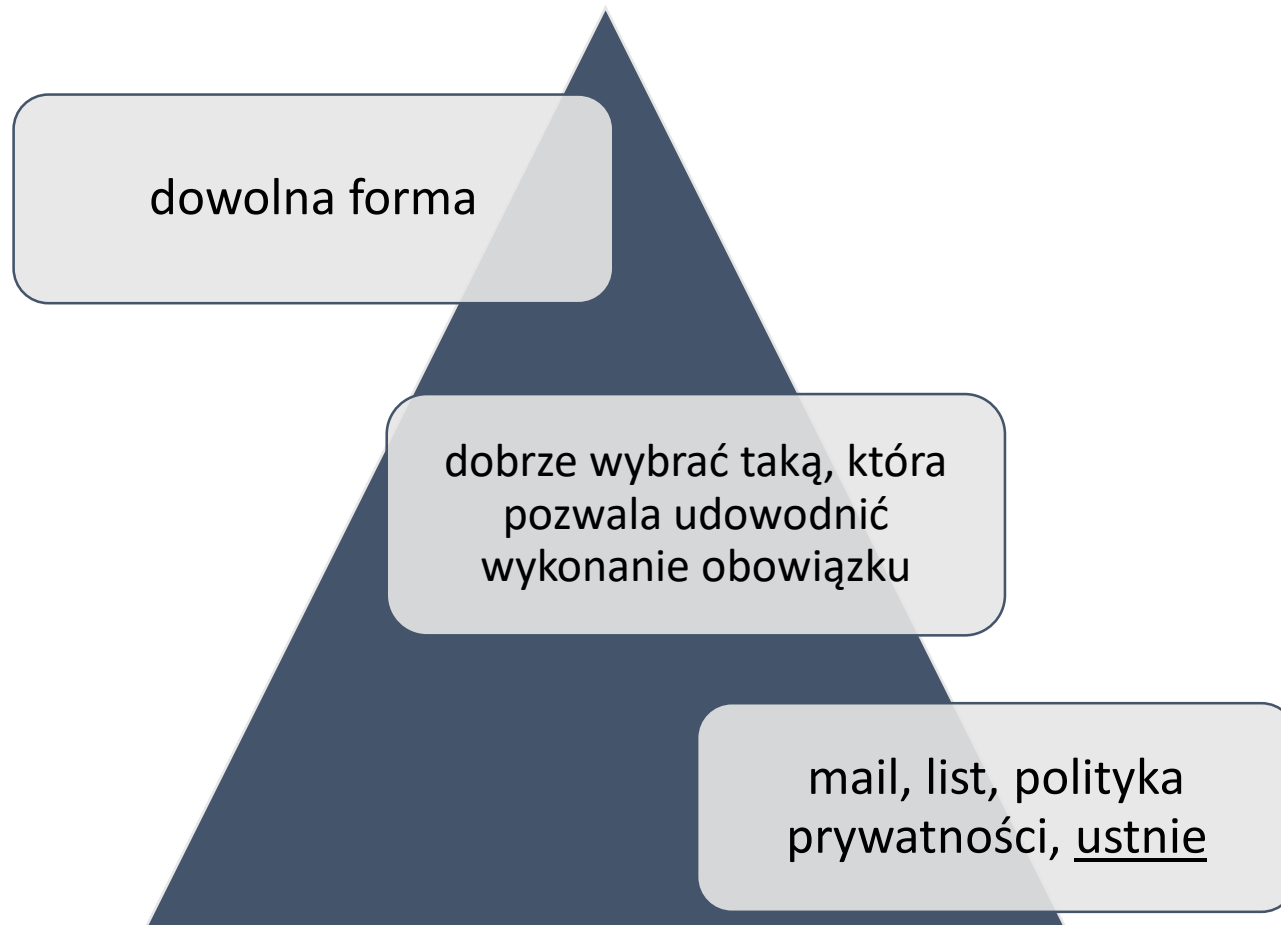
Wtórne zbieranie danych – podawane informacje:

- tożsamość ADO i dane kontaktowe oraz dane kontaktowe inspektora ochrony danych
- cele przetwarzania danych osobowych oraz podstawa prawna
- kategorie pozyskanych danych
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców
- informacje o zamiarze przekazywania danych do państw trzecich
- okres przechowywania danych
- uzasadnione interesy ADO lub podmiotu trzeciego
- informacje o uprawnieniach podmiotu danych (w tym o cofnięciu zgody)
- prawo wniesienia skargi do organu nadzorczego
- źródło pochodzenia danych
- dobrowolność lub obowiązek podania danych + konsekwencje ich niepodania
- informacje o zautomatyzowanym podejmowaniu decyzji
- planowana zmiana celu

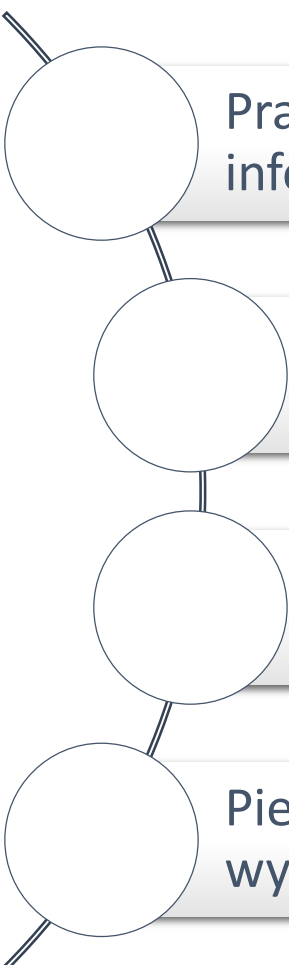
Obowiązek informacyjny – art. 14



Sposoby realizacji obowiązku informacyjnego



Prawo dostępu do danych



Prawo uzyskania potwierdzenia czy i jakie dane są przetwarzane + informacje analogiczne do zakresu obowiązków informacyjnych

Administrator dostarcza podmiotowi danych KOPIĘ danych podlegających przetwarzaniu

Możliwość udzielania odpowiedzi elektronicznie

Pierwsza kopia danych – bezpłatna, dalsze – opłata w rozsądnej wysokości

Przesłanki prawa do usunięcia danych

Dane nie są już niezbędne do celów, w których zostały zebrane

Podmiot danych cofnął zgodę, na której opierało się przetwarzanie i nie ma innej podstawy dla przetwarzania

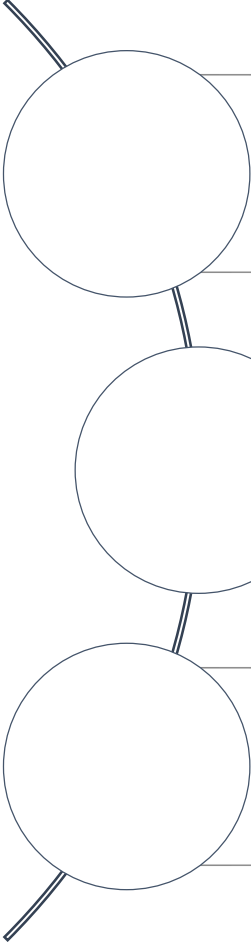
Wniesiono sprzeciw słabszy i nie ma nadrzędnych prawnie uzasadnionych podstaw dla przetwarzania lub sprzeciw mocniejszy

Dane osobowe były przetwarzane niezgodnie z prawem

Dane osobowe muszą być usunięte w celu wywiązania się z obowiązku prawnego

Dane osobowe zebrano w związku z oferowaniem usług społeczeństwa informacyjnego dziecku na podstawie jego zgody

Prawo do bycia zapomnianym



Jeżeli administrator upublicznił dane osobowe i ma obowiązek ich usunięcia

Podejmuje **rozsądne** działania, by poinformować innych administratorów przetwarzających te dane o konieczności usunięcia łącznie z tych danych, ich kopii lub replikacji

Bierze się pod uwagę koszty realizacji i dostępną technologię



lubasz&wspólnicy

KANCELARIA RADCÓW PRAWNYCH

Prawo do niepodlegania profilowaniu

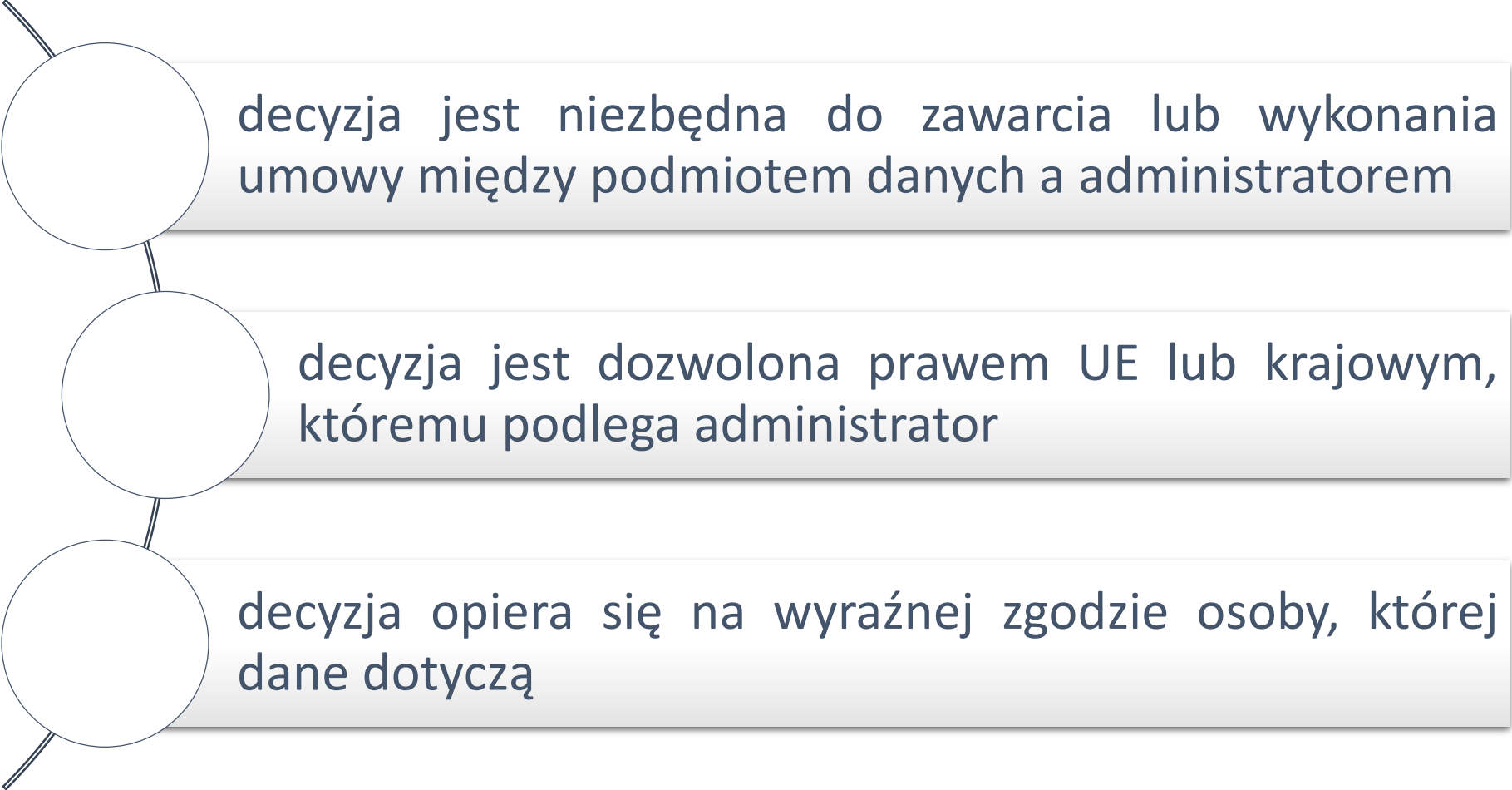
Zautomatyzowanego podejmowania decyzji

- w tym profilowania
- profilowanie polega na wykorzystaniu danych osobowych do oceny niektórych czynników człowieka

Decyzja musi wywoływać wobec człowieka

- skutki prawne
- w inny podobny sposób istotnie nań wpływa

Wyjątki od prawa do niepodlegania profilowaniu



decyzja jest niezbędna do zawarcia lub wykonania umowy między podmiotem danych a administratorem

decyzja jest dozwolona prawem UE lub krajowym, któremu podlega administrator

decyzja opiera się na wyraźnej zgodzie osoby, której dane dotyczą

Gwarancje profilowania

nie może opierać się na danych szczególnej kategorii

- zgoda lub niezbędność przetwarzania ze względów na ważny interes publiczny
- właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów

niestosowanie takiego przetwarzania wobec dzieci

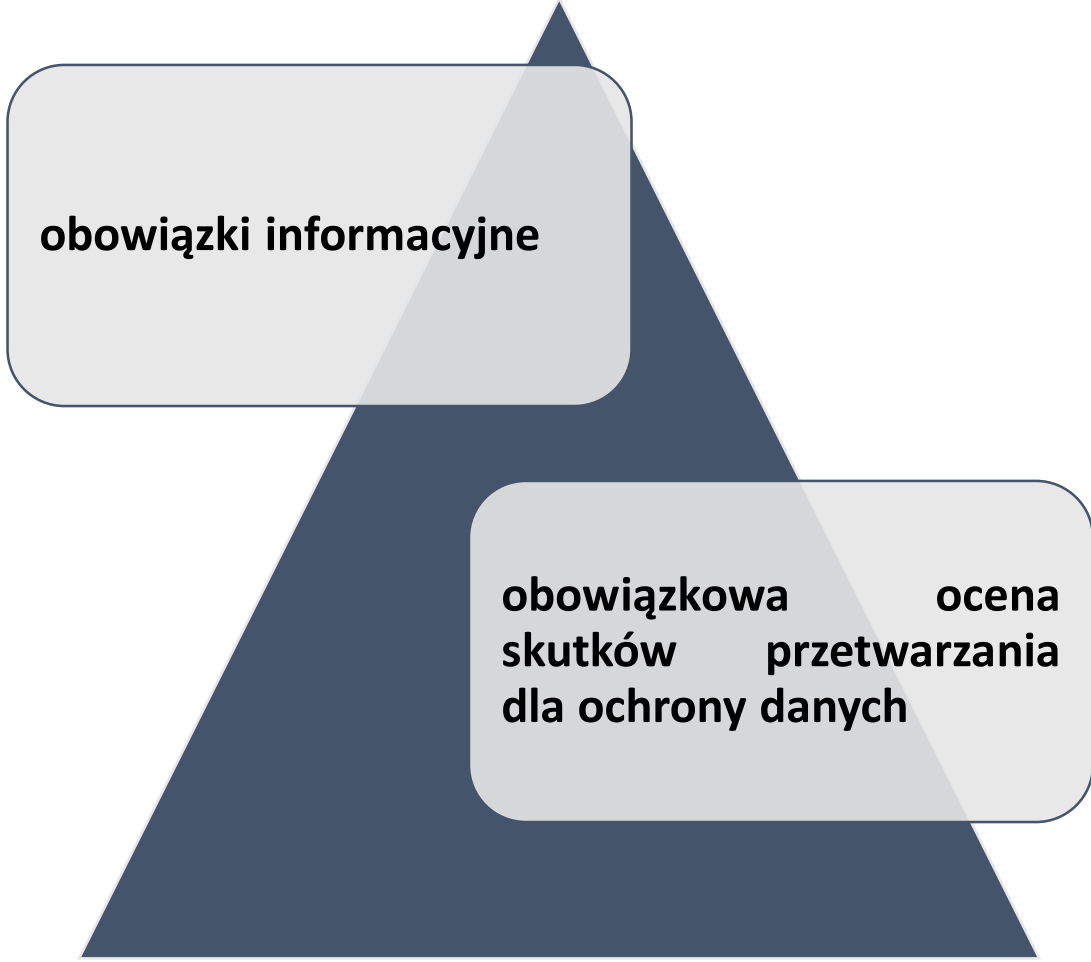
prawo do własnego stanowiska i zakwestionowania decyzji do człowieka

odpowiednie matematyczne i statystyczne procedury profilowania

dbanie o poprawność danych w celu zmniejszenia ryzyka błędów

zapobieganie dyskryminacji

Dodatkowe obowiązki związane z profilowaniem



obowiązki informacyjne

**obowiązkowa ocena
skutków przetwarzania
dla ochrony danych**

Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przelać te dane innemu administratorowi bez przeszkód ze strony administratora, któremu dane te dostarczono, jeżeli:

przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy

przetwarzanie odbywa się w sposób zautomatyzowany.

Jakich danych dotyczy to prawo

Danych osobowych

- przekazanych aktywnie i świadomie przez podmiot danych
- tzw. danych „zaobserwowanych”, które są przekazywane administratorowi wraz z korzystaniem z określonej usługi lub urządzenia

Uprawnienia

Prawo do otrzymania danych osobowych

Prawo do przestania danych innemu administratorowi

Prawo do żądania, przestania danych do nowego administratora

- o ile jest to technicznie możliwe

Prawo do sprzeciwu

Możliwość złożenia sprzeciwu

- w dowolnym momencie
- w przypadku przetwarzania danych: w interesie publicznym, w ramach sprawowania władzy publicznej lub w uzasadnionych interesach

Skutek -> niemożność dalszego przetwarzania

- chyba, że administrator wykaże istnienie ważnych, uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności podmiotu danych

W przypadku przetwarzania w celach marketingu bezpośredniego

- możliwość złożenia sprzeciwu zawsze
- brak możliwości przetwarzania pierwotnego lub dalszego

Obowiązki Administratora

Nowe obowiązki administratorów

**Ogólny obowiązek
zapewnienia
zgodności**

**Privacy by design
Privacy by default**

Dokumentacja

**Bezpieczeństwo
przetwarzania**

*Privacy risk
assessment*

**Ocena skutków
przetwarzania**

*Data protection
impact assessment*

**Zgłoszenie
naruszenia**

Ogólny obowiązek zabezpieczenia danych

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 RODO i aby móc to wykazać

Środki te są w razie potrzeby poddawane przeglądom i uaktualniane

Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych

Privacy by Design i Privacy by Default

Uwzględnienie ochrony danych w fazie projektowania

- administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania -wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

Domyślna ochrona danych

- Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania

Ocena skutków dla ochrony danych

Jeżeli dany rodzaj przetwarzania



ze względu na swój charakter, zakres, kontekst i cele



z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych,



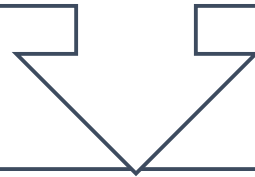
administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.



lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

Upřednie konsultacje

Jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka,



to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

Dokumentacja

Rejestrowanie czynności przetwarzania

- ADO prowadzi rejestr podlegających mu czynności przetwarzania danych osobowych.
- W rejestrze tym zamieszcza się następujące informacje:
 - imię i nazwisko lub nazwę oraz dane kontaktowe ADO oraz wszelkich współadministratorów, przedstawiciela administratora oraz DPO;
 - cele przetwarzania;
 - opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
 - kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
 - planowane terminy usunięcia poszczególnych kategorii danych;
 - ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

W przypadku naruszenia ODO, ADO bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż 72 h po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu

chyba że jest mało prawdopodobne, by naruszenie to skutkowało zagrożeniem dla praw i wolności osób fizycznych

do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia

Zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

Jeżeli naruszenie ochrony danych osobowych może nieść duże zagrożenie dla praw i wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia podmiot danych o takim naruszeniu.

Zawiadomienie napisane jasnym i prostym językiem

Zawiadomienie nie jest wymagane, jeżeli:

- ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych, których dotyczy naruszenie;
- ADO przedsięwziął następnie środki eliminujące prawdopodobieństwo dużego zagrożenia dla praw i wolności osoby, której dane dotyczą,
- lub wymagałoby ono niewspółmiernie dużego wysiłku.

Dziękuję za uwagę!



Witold Chomiczewski, LL.M.

wspólnik, radca prawny

witold.chomiczewski@lubasziwspolnicy.pl

TT: @wchomiczewski

tel.: +48 503 027 760

Lubasz i Wspólnicy - Kancelaria
Radców Prawnych sp. k.

ul. Żwirki 17
90-539 **Łódź**
+ 48 42 631 94 44

Biurowiec Spektrum, piętro 25,
ul. Twarda 18
00-105, **Warszawa**
+ 48 22 526 55 20



pl-pl.facebook.com/lubaszlawspolnicy/



pl.linkedin.com/company/lubasz-i-wspolnicy-law-firm



twitter.com/liwlegal