Ochrona danych osobowych

r.pr. Monika Susałko

Lubasz i Wspólnicy Kancelaria Radców Prawnych
monika.susalko@lubasziwspolnicy.pl

ROZPORZĄDZENIE OGÓLNE – PERSPEKTYWA ZMIAN

Rozporządzenie PE i Rady UE

- **Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)**

Cele rozporządzenia

Wysoki i spójny poziom ochrony osób fizycznych

Usunięcie przeszkód w przepływie danych osobowych

Pewność i przejrzystość prawa dla mikroprzedsiębiorców i MŚP

Ujednolicenie poziomu prawnie egzekwowalnych praw

Ujednolicenie poziomu obowiązków i zadań ADO i procesorów

Dane osobowe

wszelkie **informacje**

zidentyfikowanej I **możliwej do zidentyfikowania**

bezpośrednio
pośrednio

Dane szczególnych kategorii

- dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych,
- dane genetyczne (art. 4 pkt. 13 RODO),
- dane biometryczne (art. 4 pkt. 14 RODO),
- dane dotyczące zdrowia (art. 4 pkt. 15 RODO),
- dane dotyczące seksualności i orientacji seksualnej.

Przetwarzanie danych dot. wyroków skazujących i naruszeń prawa

Przetwarzanie

Gromadzenie	Utrwalanie	Organizowanie	Porządkowanie
Przechowywanie	Adaptowanie / modyfikowanie	Pobieranie	Przeglądanie
Wykorzystywanie	Ujawnianie	Dopasowywanie / łączenie	Rozpowszechnianie
	Ograniczanie	Usuwanie / niszczenie	

Administrator danych

osoba fizyczna lub prawna,

organ publiczny, jednostka lub inny podmiot,

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

Współadministratorzy

Co najmniej 2 ADO wspólnie ustalają cele i sposoby przetwarzania

Uzgodnienia zgodnie z faktyczną rolą każdego ADO

- 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 ADO
- Przeciwko każdemu ADO

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.

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

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

Administrator i podmiot przetwarzający

OBOWIĄZKI

Nowe obowiązki administratorów

Bezpieczeństwo przetwarzania

Privacy risk assessment

Privacy by design

Privacy by default

Ogólny obowiązek wdrożeniowy

Dokumentacja

Ocena skutków przetwarzania

Privacy impact assessment

Zgłoszenie naruszenia

Ogólny obowiązek

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.

Bezpieczeństwo przetwarzania

ADO i procesor wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiadający ryzyku – uwzględniając

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

Ocena skutków dla ochrony danych jest obligatoryjna 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, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub**
- **systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.**

Rejestrowanie czynności przetwarzania

ADO prowadzi rejestr czynności przetwarzania, za które odpowiada

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;

Obowiązki

Współpraca z organem nadzorczym

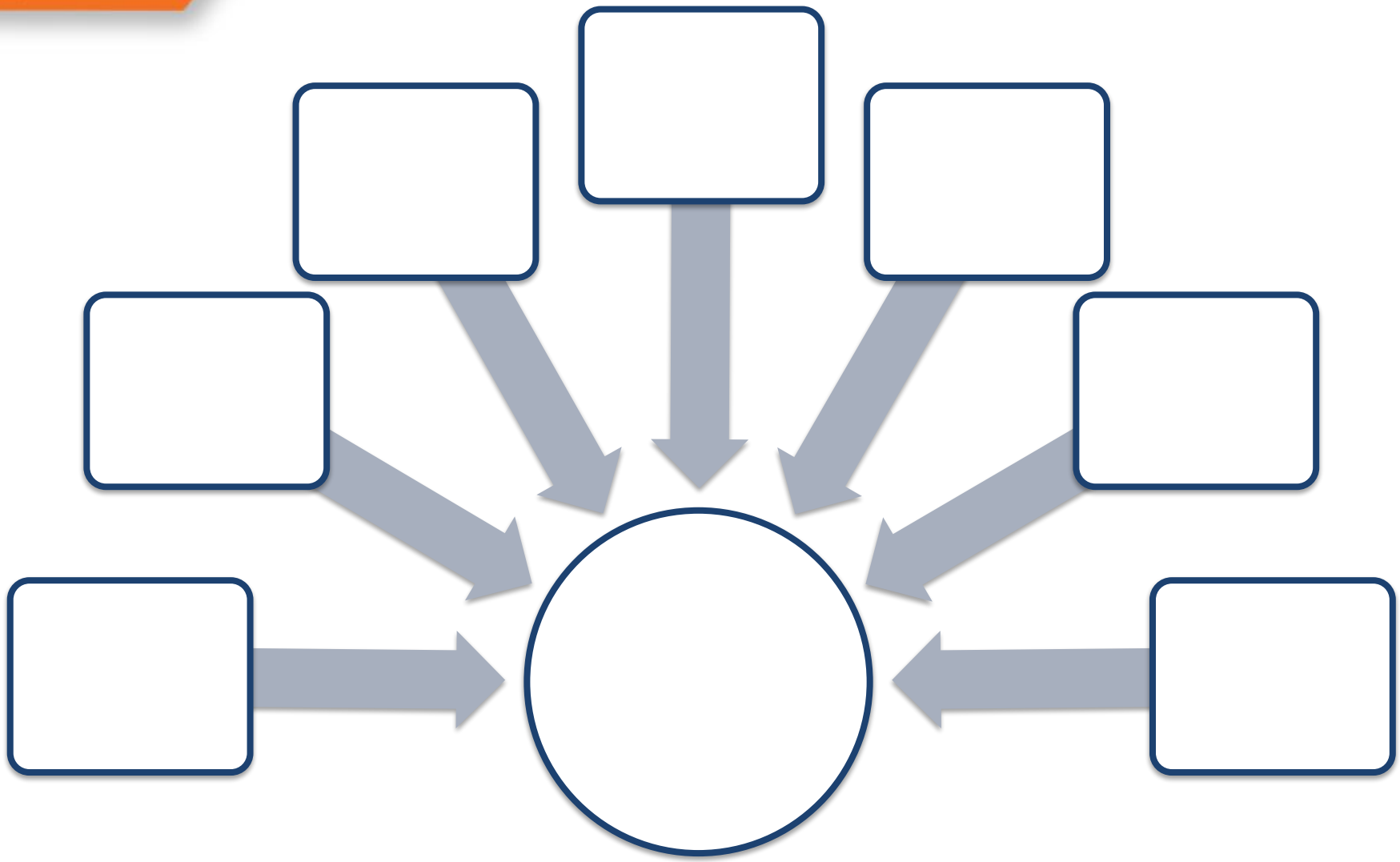
- Administrator i podmiot przetwarzający oraz – jeżeli istnieje – przedstawiciel administratora lub podmiotu przetwarzającego
- na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań.

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



Powierzenie

Możliwość korzystania z usług procesora

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

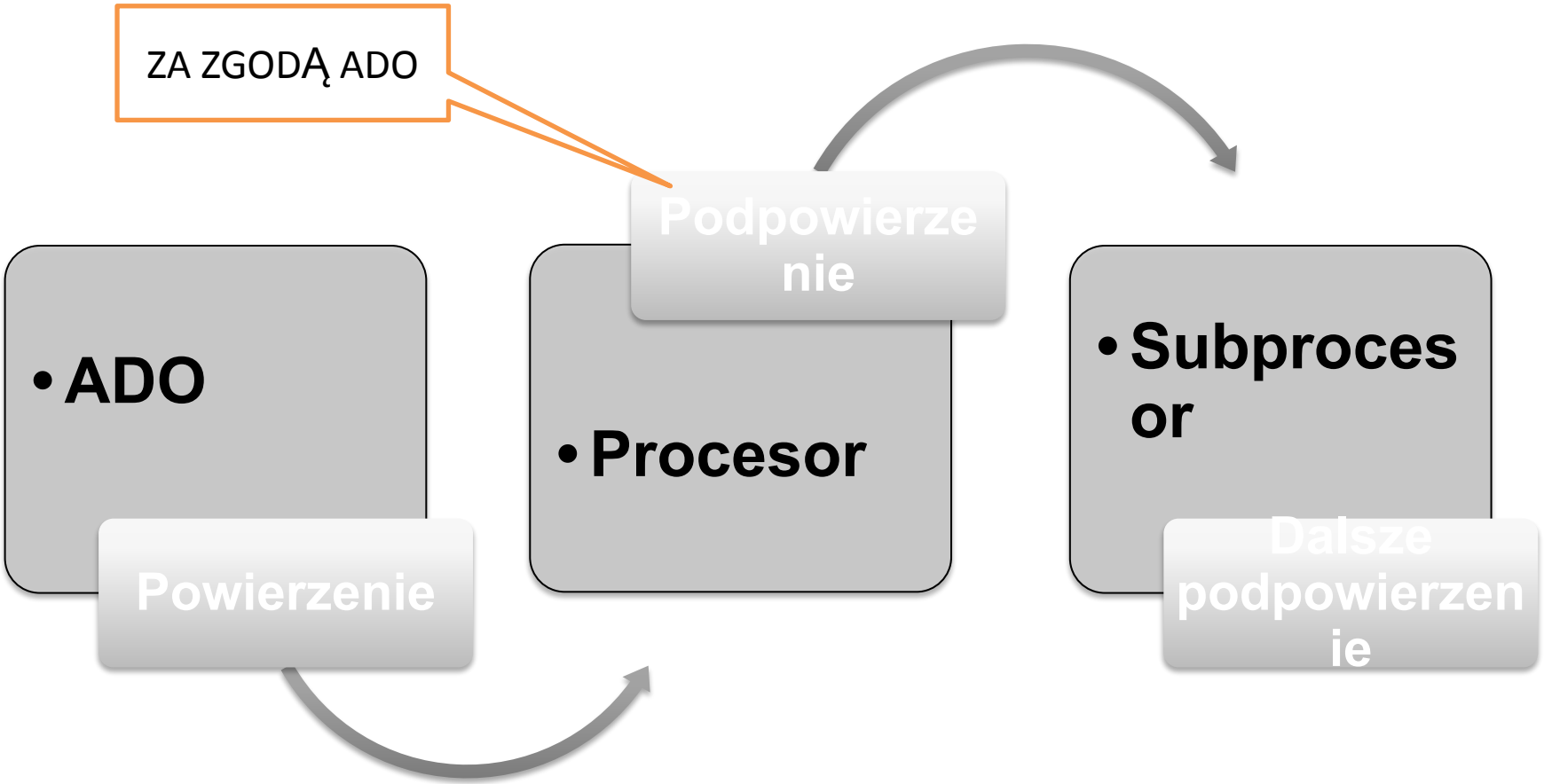
Przetwarzanie danych przez podmiot przetwarzający

- Regulowane **umową**
- Lub **innym instrumentem prawnym**

Wymogi dla umowy

- Przedmiot i czas (okres) przetwarzania
- Charakter i cel przetwarzania
- Rodzaj DO i kategorie osób
- Obowiązki i prawa ADO

Możliwość dokonywania dalszych powierzeń



Inspektor ochrony danych

Inspektor ochrony danych

Obligatoryjne powołanie inspektora ochrony danych (DPO), gdy:

- przetwarzania dokonuje 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 danych osobowych szczególnych kategorii, a także danych o wyrokach skazujących i o przestępstwach.

Inspektor ochrony danych

Pozostali ADO

- fakultatywność powołania DPO

Grupa przedsiębiorstw

- możliwość wyznaczenia jednego inspektora ochrony danych dla grupy, pod warunkiem, że będzie można nawiązać z nim kontakt z każdej jednostki

Organy lub podmioty publiczne

- możliwość wyznaczenia jednego inspektora ochrony danych dla kilku takich organów lub podmiotów, z uwzględnieniem ich struktury organizacyjnej i wielkości

Zadania inspektora ochrony danych – art. 39

informowanie ADO lub podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i doradzanie im w tej sprawie;

monitorowanie przestrzegania RODO oraz strategii ADO lub podmiotu przetwarzającego w dziedzinie ODO;

udzielanie porad na żądanie co do oceny skutków pod kątem ochrony danych oraz monitorowanie jej wykonania ;

współpraca z organem nadzorczym;

pełnienie funkcji punktu kontaktowego wobec organu nadzorczego;

Pełnienie funkcji punktu kontaktowego dla podmiotów danych

Prawa podmiotu danych

Obowiązek informacyjny

Dwa rodzaje

- **Informacje podawane OBOWIĄZKOWO w przypadku gromadzenia danych od podmiotu danych – art. 13**
- **Informacje podawane w przypadku pozyskiwania danych w sposób inny niż od osoby, której dane dotyczą – art. 14**

Obowiązek informacyjny – art. 13

Bezpośrednie zbieranie danych – podawane informacje:

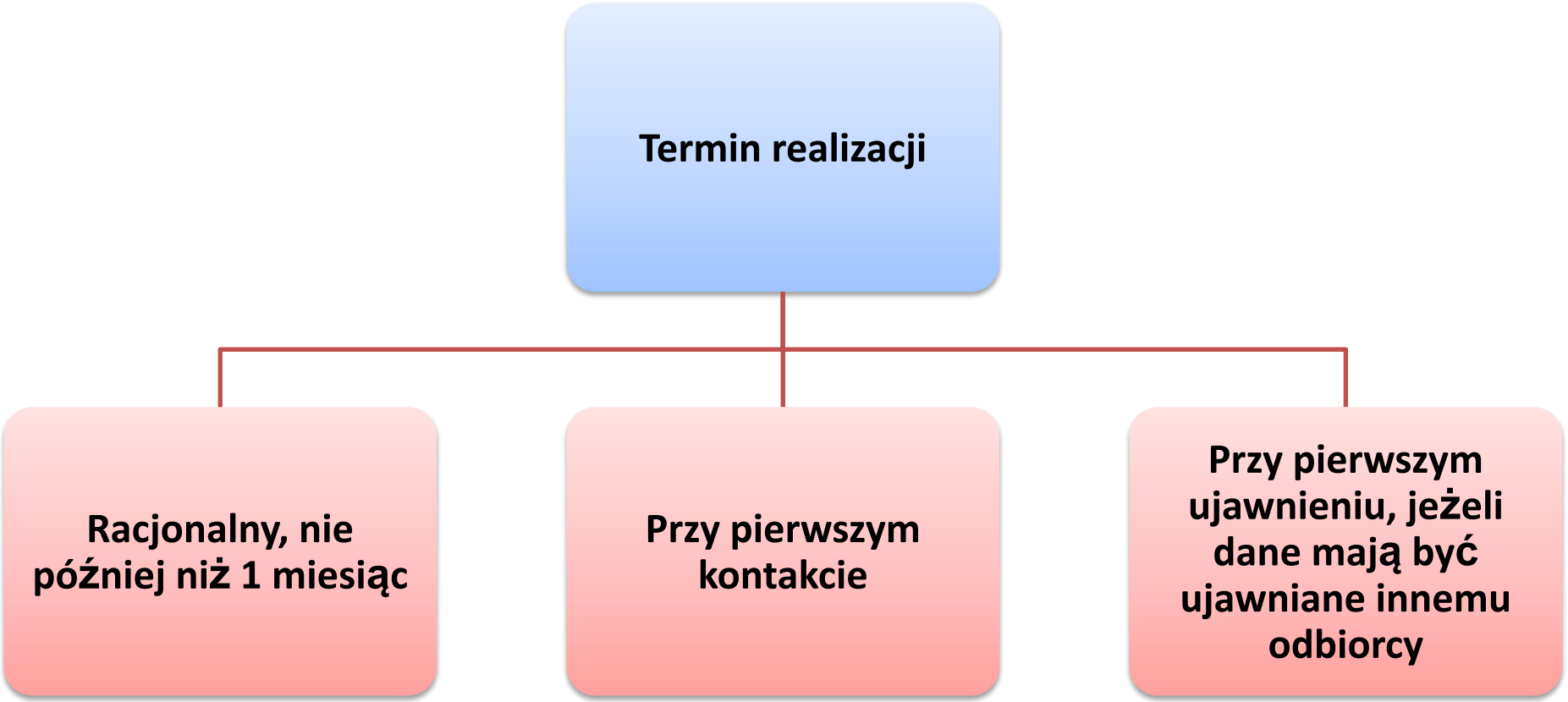
- tożsamość ADO i dane kontaktowe oraz dane kontaktowe inspektora ochrony danych
- cele przetwarzania danych osobowych oraz podstawa prawna
- uzasadnione interesy realizowane przez administratora lub przez stronę trzecią
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców
- informacje 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

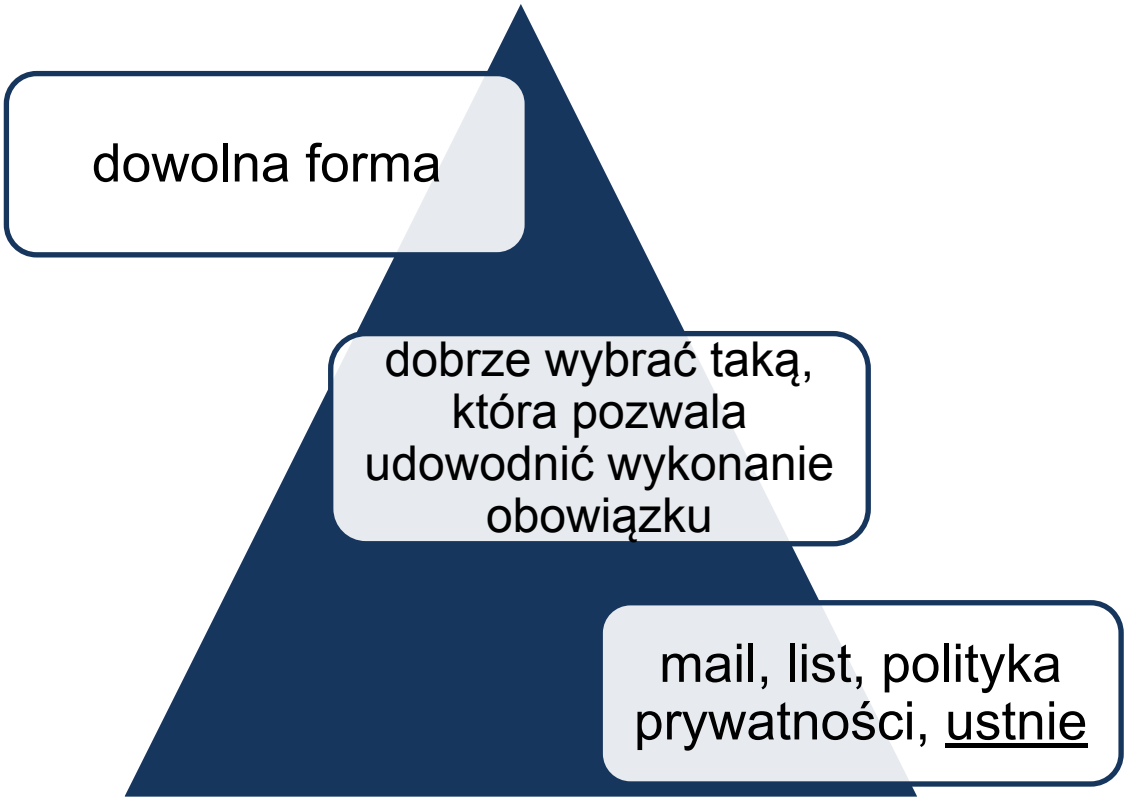
Wtórne zbieranie danych – podawane informacje:

- 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

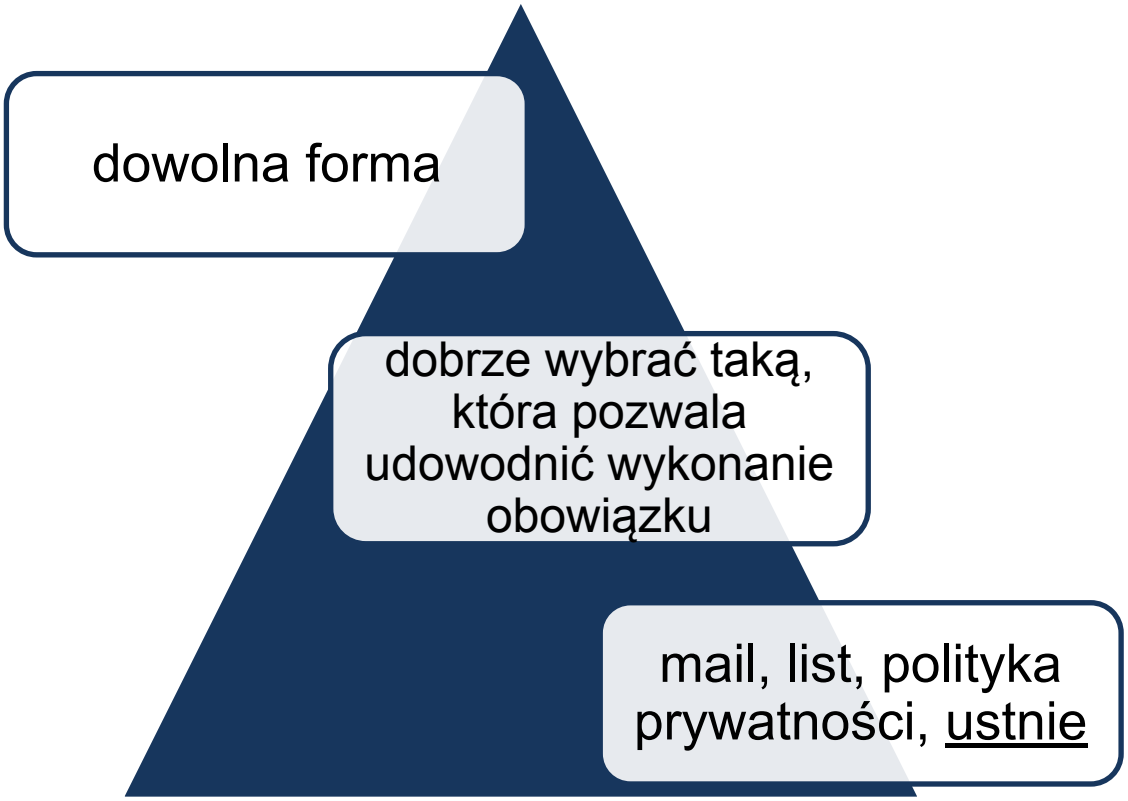


Termin realizacji wniosków z art. 15-22

Administrator bez zbędnej zwłoki – najpóźniej w terminie miesiąca od otrzymania wniosku – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z wnioskiem na podstawie art. 15–22 RODO.

Jeżeli administrator nie w/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.

Sposoby realizacji obowiązku informacyjnego



Prawo dostępu do danych – art. 15

- Prawo uzyskania potwierdzenia czy i jakie dane są przetwarzane + informacje analogiczne do zakresu obowiązków informacyjnych
- ADO dostarcza podmiotowi danych KOPIĘ danych podlegających przetwarzaniu
- Możliwość udzielania odpowiedzi elektronicznie
- Pierwsza kopia danych – bezpłatna, dalsze – opłata w rozsądnej wysokości

Prawo do bycia zapomnianym – art. 17

Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego usunięcia dotyczących jej DO, a ADO ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- dane nie są już niezbędne do celów, w których zostały zgromadzone lub w inny sposób przetworzone;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania danych;
- osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania danych osobowych i nie występują nadrzędne uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania danych osobowych;
- dane były przetwarzane niezgodnie z prawem;
- dane muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie krajowym, któremu podlega administrator;
- dane zostały zgromadzone w związku z oferowaniem usług społeczeństwa informacyjnego dzieciom.

Prawo do ograniczenia przetwarzania – art. 18

Możliwość żądania ograniczenia przetwarzania, jeżeli:

ADO nie

Prawo do przenoszenia danych – art. 20

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 przesłać 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.

Prawo do sprzeciwu – art. 21

Możliwość złożenia sprzeciwu

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

Skutek -> niemożność dalszego przetwarzania danych przez ADO

- chyba, że ADO 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

Ograniczenie profilowania – art. 22

Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, chyba, że decyzja:

- **jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a ADO;**
- **jest dozwolona prawem UE lub pr. krajowym, któremu podlega ADO;**
- **opiera się na wyraźnej zgodzie osoby, której dane dotyczą.**

ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ I SANKCJE

Prawo do wniesienia skargi

osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego,

w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia

jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczących nie jest zgodne z RODO

Postępowanie przed organem nadzorczym

Zgodnie z projektem ustawy o ochronie danych:

- Organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych,
- Postępowanie jednoinstancyjne - podstawą KPA z uwzględnieniem odmienności przewidzianych w ustawie
- Postępowanie dowodowe – tłumaczenie dokumentów, zastrzeżenie tajemnicy przedsiębiorstwa,
- Uprawnienie PUODO do nakładania grzywny przymuszającej w trakcie postępowania
- Możliwość wydawania zaskarżalnych postanowień tymczasowych,
- Skarga na decyzję PUODO do sądu administracyjnego,
- Wniesienie skargi do sądu administracyjnego wstrzymuje wykonanie decyzji PUODO w zakresie kary finansowej.

Administracyjne kary pieniężne

Możliwość nakładania kar – organ nadzorczy

Nałożenie kary i jej wysokość:

- Zależne od okoliczności
- Oceniane indywidualnie
- Stosowane obok lub zamiast środków określonych w art. 58 ust. 2 RODO

Administracyjne kary pieniężne

Okoliczności, które mają być uwzględnione przy ustalaniu kary

- **charakter, waga i czas trwania naruszenia w określonym kontekście przetwarzania;**
- **umyślny lub nieumyślny charakter naruszenia;**
- **działania ADO lub procesora w celu minimalizacji szkody poniesionej przez podmiot danych;**
- **stopień odpowiedzialności ADO lub procesora;**
- **wcześniejsze naruszenia ze strony ADO lub procesora;**
- **stopień współpracy z organem nadzorczym;**
- **kategorie danych osobowych, których dotyczyło naruszenie;**
- **sposób, w jaki organ nadzorczy dowiedział się o naruszeniu;**
- **przestrzeganie wcześniej zastosowanych wobec ADO lub procesora środków;**
- **stosowanie zatwierdzonych kodeksów postępowania;**
- **wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy.**

Administracyjne kary pieniężne

Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie administracyjnej karze pieniężnej w wysokości do:			
10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 %	lub	20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 %	jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa:

Kary niższe - za naruszenia

obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 oraz 43;

obowiązków podmiotu certyfikującego, o których mowa w art. 42 oraz 43;

obowiązków podmiotu monitorującego, o których mowa w art. 41 ust. 4;

Kary wyższe - za naruszenia

podstawowych zasad przetwarzania, w tym warunków zgody;

praw osób, których dane dotyczą;

przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej;

wszelkich obowiązków wynikających z prawa krajowego przyjętego na podstawie rozdziału IX;

nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1.