Ochrona
danych osobowych
Podstawowe pojęcia i informacje

Dane osobowe (art. 4 ust. 1 RODO)

Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą).

Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak:

- imię i nazwisko,
- numer identyfikacyjny,
- dane o lokalizacji,
- Identyfikator internetowy lub
- jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane osobowe: omówienie

Dane osobowe – oznaczają informacje (…)

Informacje:

- komunikat (niezależnie od sposobu utrwalenia)
- litery, słowa, dźwięki, fotografie, zdjęcia rentgenowskie, DNA…

Dane osobowe: omówienie

Dane osobowe – oznaczają informacje (…) o osobie fizycznej

Osoba fizyczna:

- ~~KRS spółki, REGON spółki~~
- ~~nazwa osoby prawnej~~
- ~~postać fikcyjna (dr House)~~ (odmiennie aktor, który zagrał dr. House'a)
- Monika Golubska

Dane osobowe: omówienie

Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Przykłady osób zidentyfikowanych lub możliwych do zidentyfikowania:

- właściciel lokalu nr 10 przy ul. Kwiatowej w Warszawie (dane fikcyjne dla potrzeb szkoleniowych)
- wieloletni właściciel baru przy ul. Grudziądzkiej w Warszawie (dane fikcyjne dla potrzeb szkoleniowych)
- p. Zofia, pracownik PKO BP w Gdańsku przy ul. Azaliowej (dane fikcyjne dla potrzeb szkoleniowych)
- właściciel klubu „Stokrotka” na Zaspie w Gdańsku (dane fikcyjne dla potrzeb szkoleniowych)
- autor książki „Miasteczko Salem”
- Lech, laureat pokojowej Nagrody Nobla w 1983 r.
- Kasia T., blogerka, córka byłego premiera
- Tomasz P., były prezydent Miasta Gdańska
- wokalista zespołu „Dżem”
- Renata B., posłanka na Sejm IV i V kadencji,
- numer PESEL

Wymienienie imienia i nazwiska nie jest konieczne.

Dane osobowe: omówienie

Przykłady osób zidentyfikowanych lub możliwych do zidentyfikowania w UCK:

- Ordynator Kliniki Psychiatrii Dorosłych UCK
- Inspektor Ochrony Danych UCK
- Wioletta, odpowiedzialna za Zintegrowany System Zarządzania w UCK
- Edyta, pracownik Działu ds. Zarządzania Zasobami Ludzkimi UCK
- mgolubska@uck.gda.pl
- Monika, zajmuje się ochroną danych osobowych w UCK
- Dyrektor Naczelny UCK
- Jakub K., Dyrektor UCK

Tożsamość tych osób z UCK znasz lub bez problemu ustalisz.

Dane osobowe (stanowisko Organu)

Na gruncie uprzednio obowiązujących przepisów już podobnie stwierdził GIODO, że danymi osobowymi mogą być „informacje odnoszące się do każdego z aspektów życia osoby, jej życia zawodowego, prywatnego, wykształcenia, wiedzy czy cech charakteru” (decyzja GIODO z dnia 26 listopada 2009 r., Dolis/DEC-1183/09).

Czy RODO ma zastosowanie do osoby zmarłej?

Motyw 27 RODO:

RODO nie ma zastosowania do danych osobowych osób zmarłych. Państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych.

Wnioski:

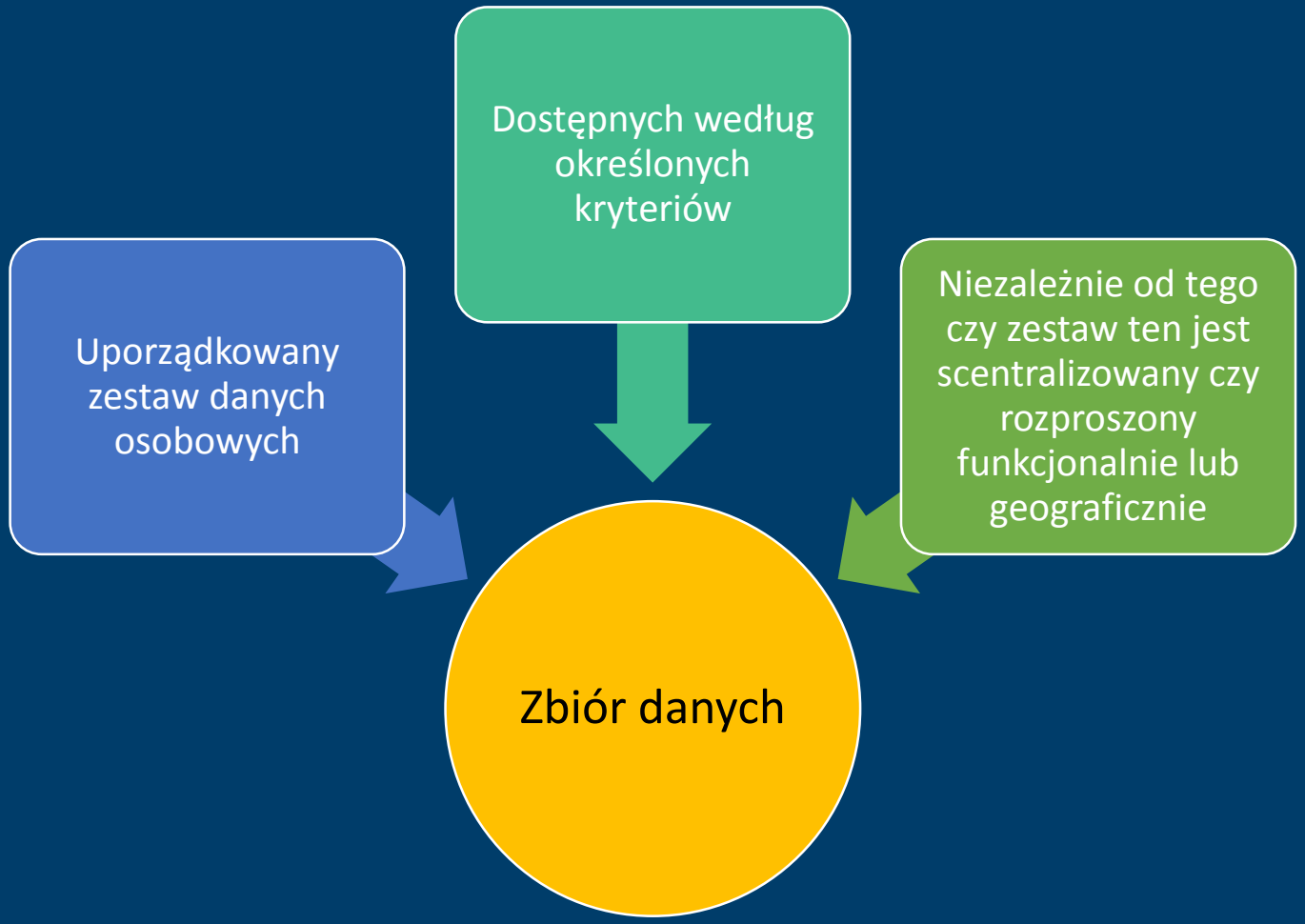
- odmowę udzielania informacji na temat osób zmarłych z powołaniem się na RODO należy uznać za nieuzasadnioną (adekwatne stanowisko wyraził GIODO na gruncie nieobowiązującej już ustawy o ochronie danych osobowych),
- w przypadku wykorzystania danych osób zmarłych (np. przesyłania ulotek reklamowych adresowanych do nieżyjącej osoby), osobom bliskim, których dobra osobiste, tj. na przykład kult pamięci o osobie zmarłej, zostały naruszone przysługuje prawo wystąpienia z powództwem cywilnym do sądu powszechnego.

Przetwarzanie (art. 4 ust. 2 RODO)

Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:

Przetwarzanie	Zbieranie	Utrwalanie	Organizowanie
Porządkowanie	Przechowywanie	Adaptowanie lub modyfikowanie	Pobieranie
Przeglądanie	Wykorzystywanie	Ujawnianie poprzez przesłanie	Rozpowszechnianie lub innego rodzaju udostępnianie
Dopasowywanie lub łączenie	Ograniczanie	Usuwanie	Niszczenie

Zbiór danych (art. 4 ust. 6 RODO)



Organ Nadzorczy (art. 4 ust. 21 RODO)

Organ Nadzorczy – oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie [UE] zgodnie z art. 51 RODO.

Np. w Polsce Prezes Urzędu Ochrony Danych Osobowych (PUODO).

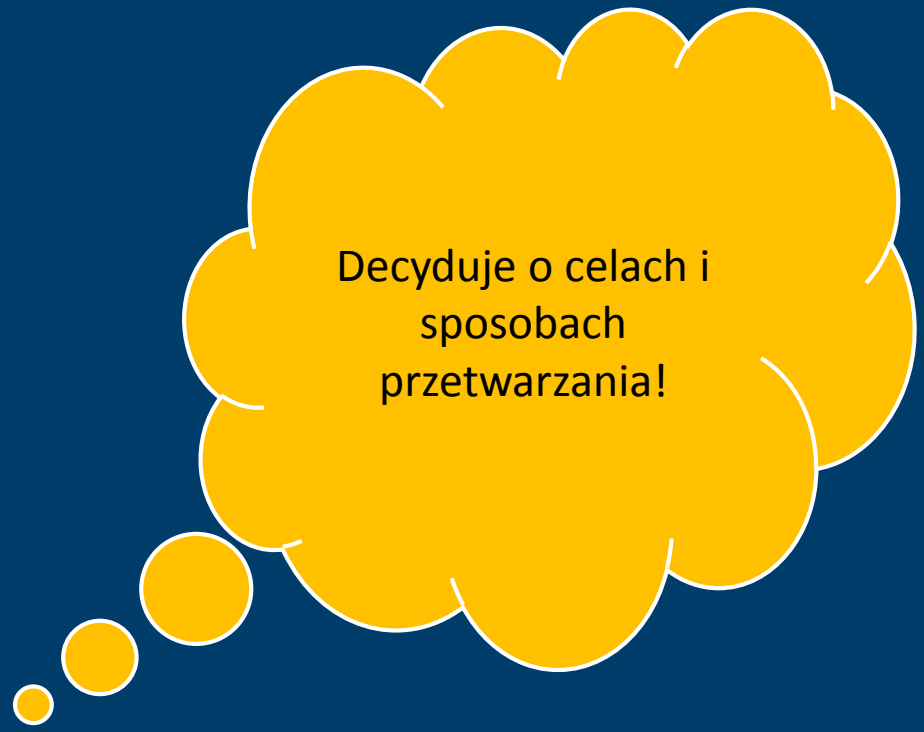
Administrator (art. 4 ust. 7 RODO)

Administrator – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (…)

Szpital

Właściciel firmy

Prezydent Miasta

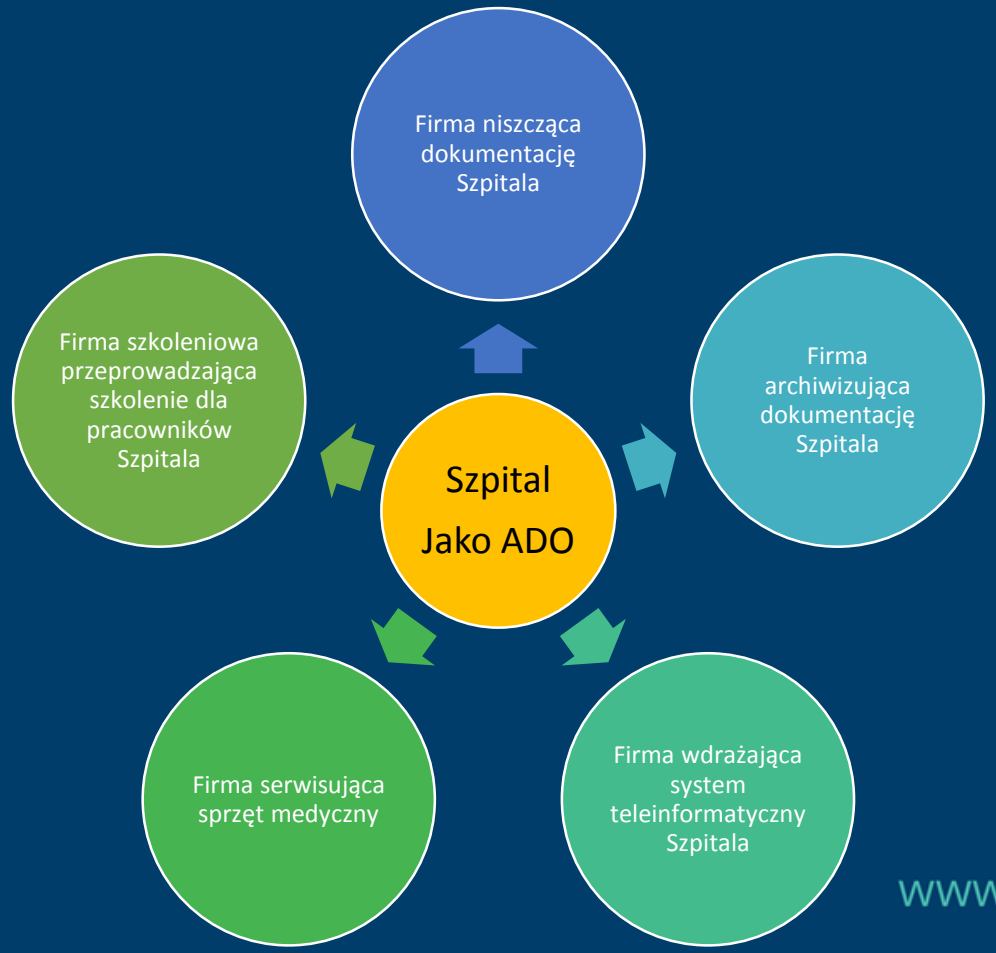


Podmiot przetwarzający (art. 4 ust. 7 RODO)

Podmiot przetwarzający (potocznie procesor) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

W imieniu administratora…

Podwykonawca!



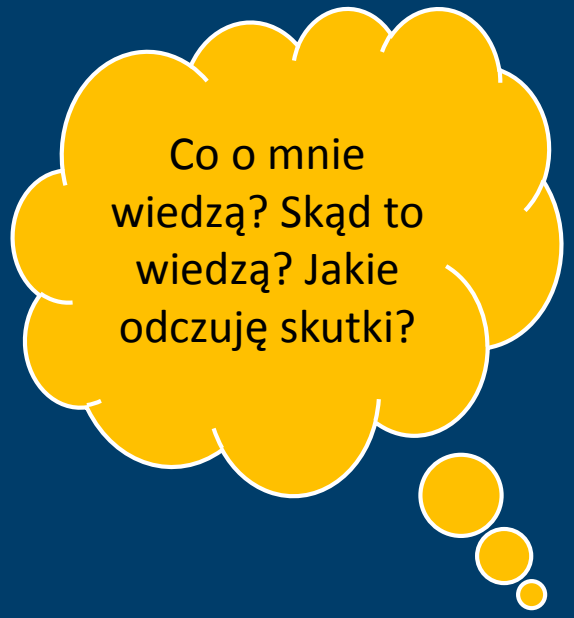
Odbiorca danych, Strona trzecia (art. 4 ust. 9 i 10 RODO)

Odbiorca (danych) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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 (…)

Strona trzecia – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

Profilowanie (art. 4 ust. 4 RODO)

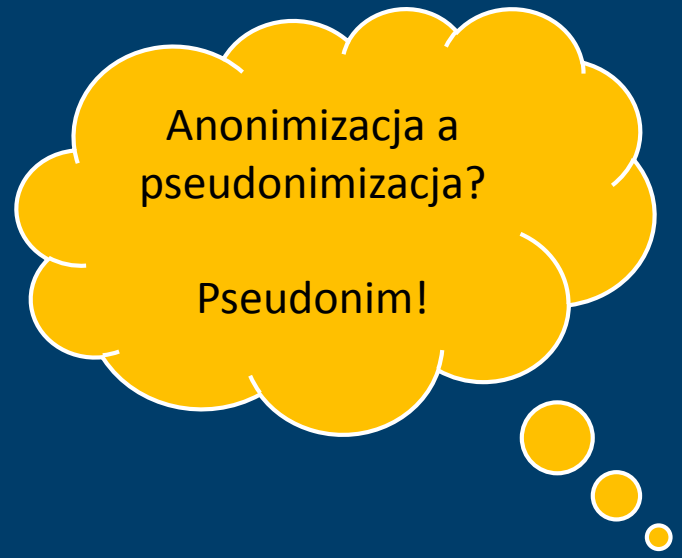
Profilowanie – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy



- aspektów dotyczących efektów pracy tej osoby fizycznej
- jej sytuacji ekonomicznej
- zdrowia
- osobistych preferencji
- zainteresowań
- wiarygodności
- zachowania
- lokalizacji
- przemieszczania się

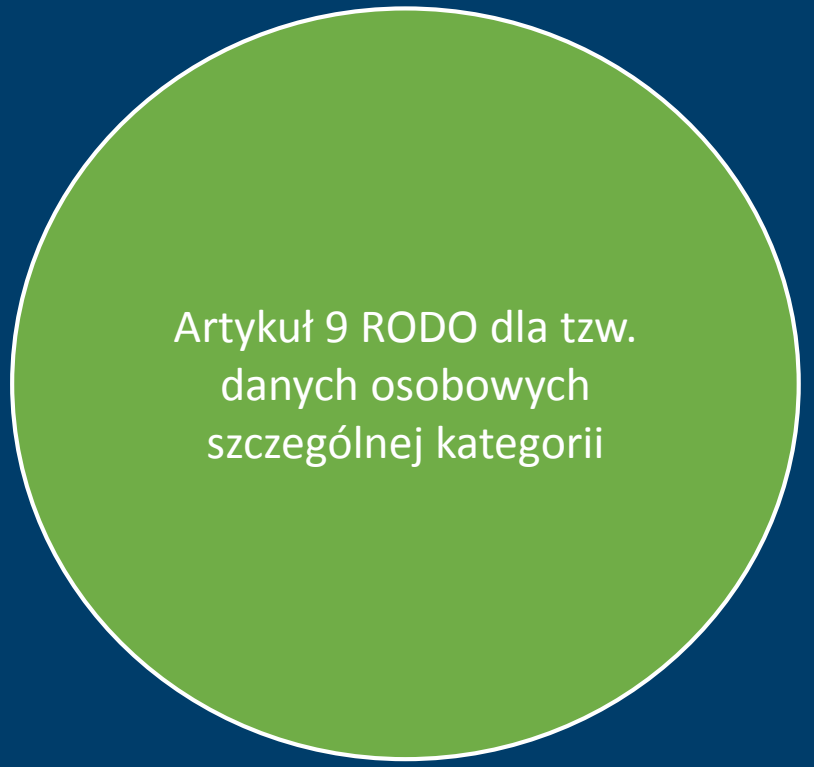
Pseudonimizacja (art. 4 ust. 5 RODO)

Pseudonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać już konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.



Dane osobowe zwykłe i szczególnej kategorii

Zgodność z prawem przetwarzania



„Zwykłe” dane osobowe (art. 6 RODO)

Art. 6 ust. 1 RODO: Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie (…)
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem

Dane osobowe szczególnej kategorii (art. 9 RODO)

Art. 9 ust. 1 RODO: Zabrania się przetwarzania danych osobowych:

- ujawniających pochodzenie rasowe lub etniczne
- poglądy polityczne
- przekonania religijne lub światopoglądowe
- przynależność do związków zawodowych
- danych genetycznych
- danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej
- danych dotyczących zdrowia
- danych dotyczących seksualności lub orientacji seksualnej tej osoby

Co do zasady, zakaz przetwarzania danych szczególnej kategorii

Katalog zamknięty danych szczególnej kategorii

Dane osobowe szczególnej kategorii (art. 9 RODO)

Art. 9 ust. 2 RODO: Art. 9 ust. 1 RODO [mówiący o zakazie przetwarzania danych szczególnej kategorii] nie ma zastosowania, jeśli:

Wyłączenia zakazu przetwarzania danych szczególnej kategorii

a) osoba, której dane dotyczą wyraziła wyraźną zgodę (…), chyba że prawo Unii lub państwa członkowskiego przewidują, iż (…) nie może uchylić zakazu (…)

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonania szczególnych praw (…) w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (…)

c) przetwarzanie jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami (…)

Dane osobowe szczególnej kategorii

e) przetwarzanie dotyczy danych osobowych upublicznionych przez osobę, której dane dotyczą

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy

g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą

h) przetwarzanie jest niezbędne dla celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3 RODO.

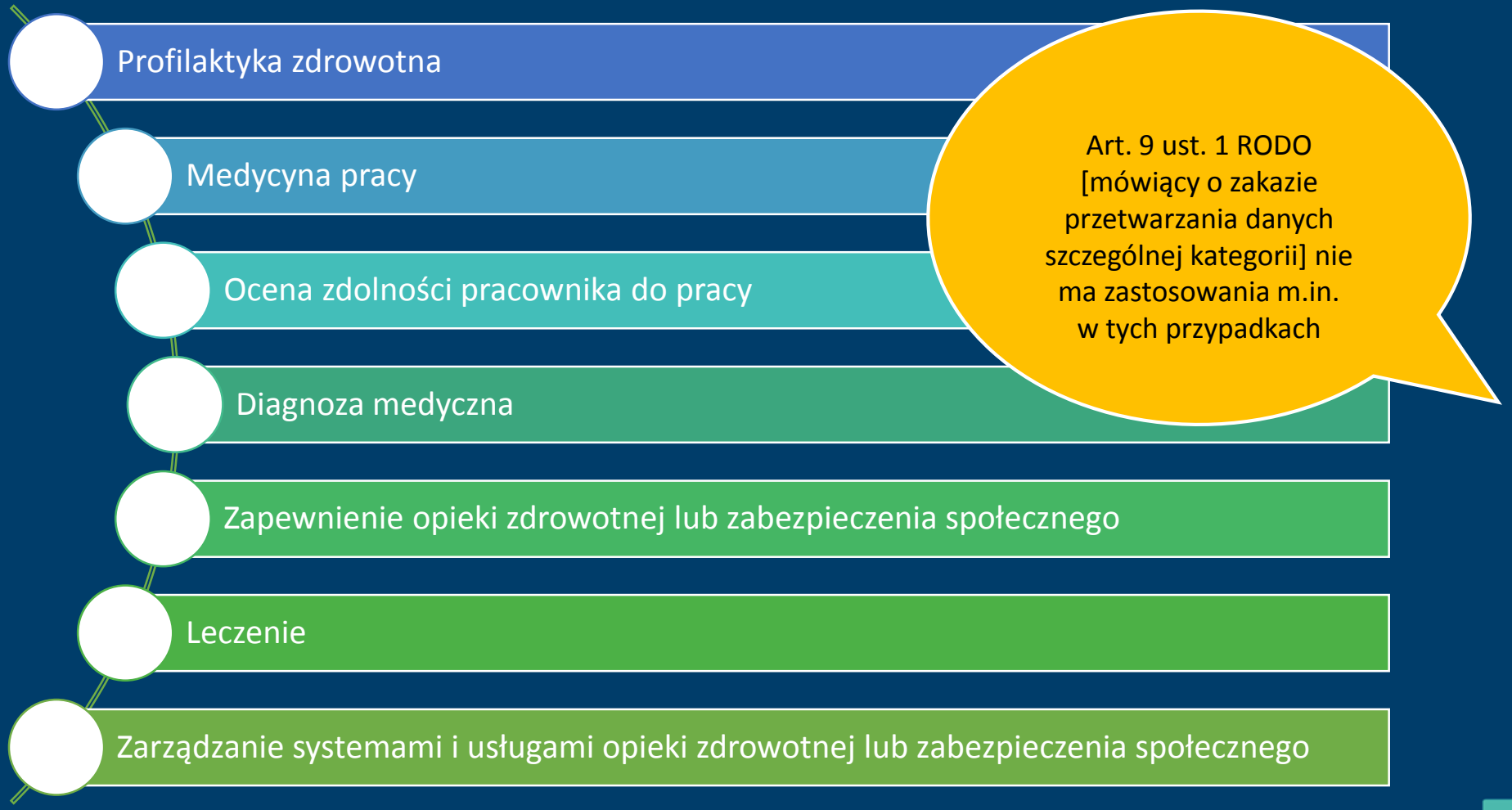
Dodatkowo nawiązanie do tego celu w artykule 9 ust. 3 RODO

Dane osobowe szczególnej kategorii

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową.

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (…)

Art. 9 ust. 2 lit. h RODO

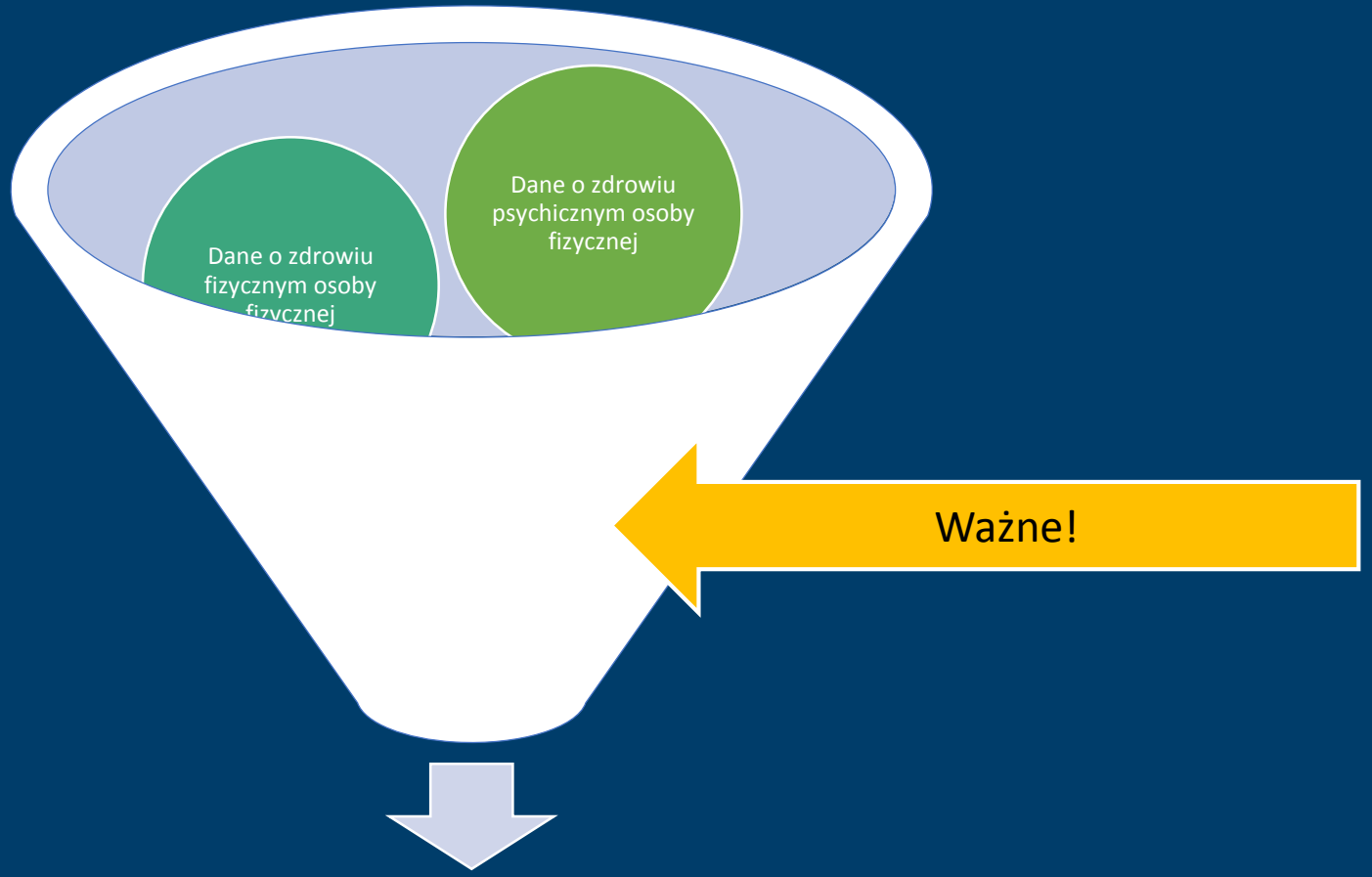


Art. 9 ust. 3 RODO

Dane osobowe, o których mowa w art. 9 ust. 1 RODO [tzw. dane osobowe szczególnej kategorii], mogą być przetwarzane do celów, o których mowa w art. 9 ust. 2 lit. h. RODO [tzw. ochrony zdrowia] jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

Błąd w tłumaczeniu polskiej wersji RODO. Błędnie wstawiono słowo „zawodowej”.

Dane dotyczące zdrowia (art. 4 ust. 15 RODO)



Dane dotyczące zdrowia

Dane dotyczące zdrowia (art. 4 ust. 15 RODO)

W tym dane o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia

Wywołanie pacjenta po nazwisku do gabinetu w Poradni Leczenia Zdrowia Psychicznego

Wywieszenie listy nazwisk pacjentów w danym dnu przyjmowanych do Poradni dermatologicznej

Udzielenie informacji, że dana osoba jest pacjentem Szpitala Onkologicznego

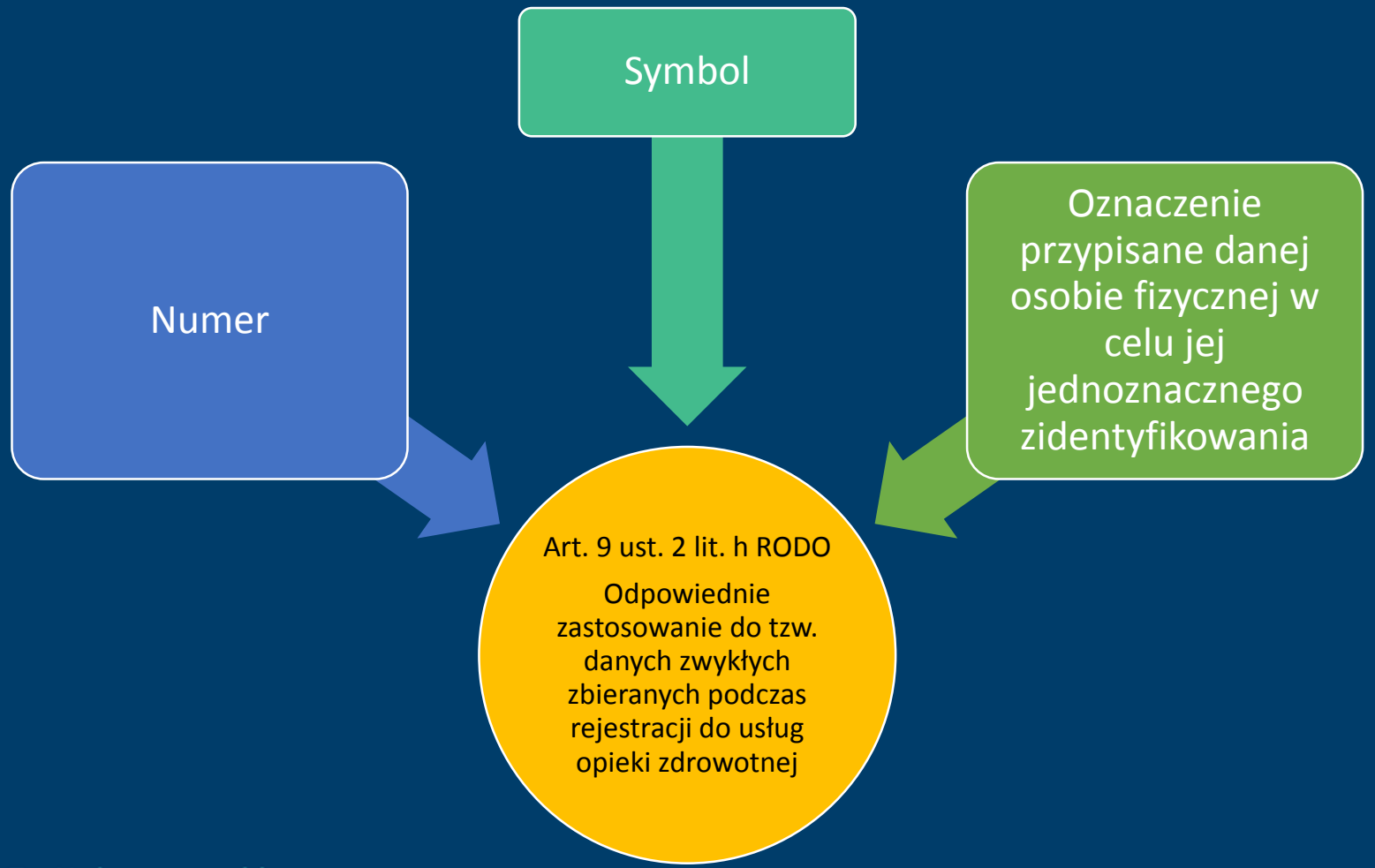
Pozostawienie dokumentacji pacjenta widocznej dla innych pacjentów w Sekretariacie Kliniki Urologii

Motyw 35 RODO

Do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą.

Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej (…), numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

Motyw 35 RODO



Dane genetyczne, dane biometryczne (art. 4 ust. 13 i 14 RODO)

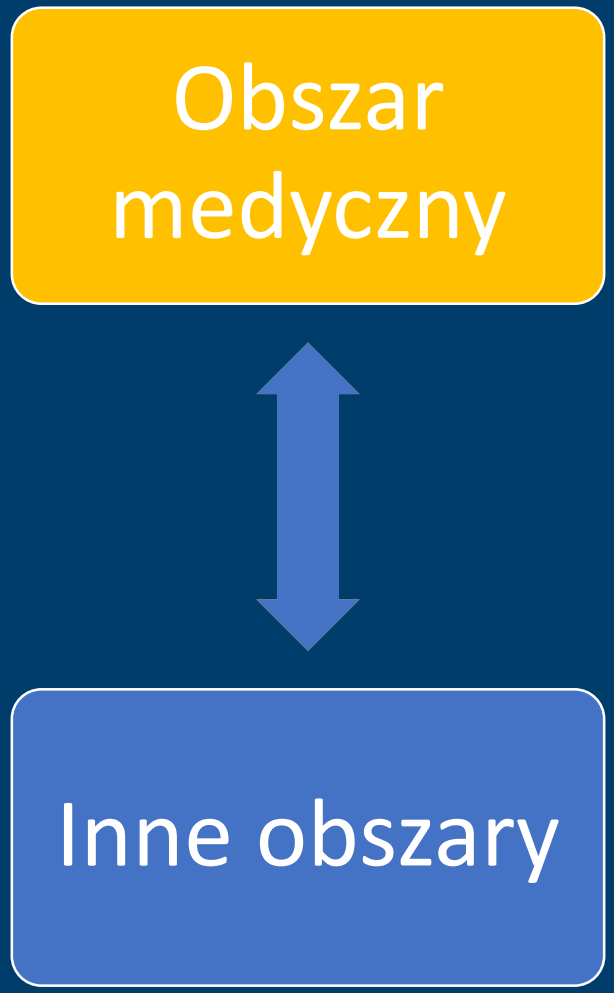
Dane genetyczne – oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

Dane biometrycze – oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

Art. 9 ust. 4 RODO

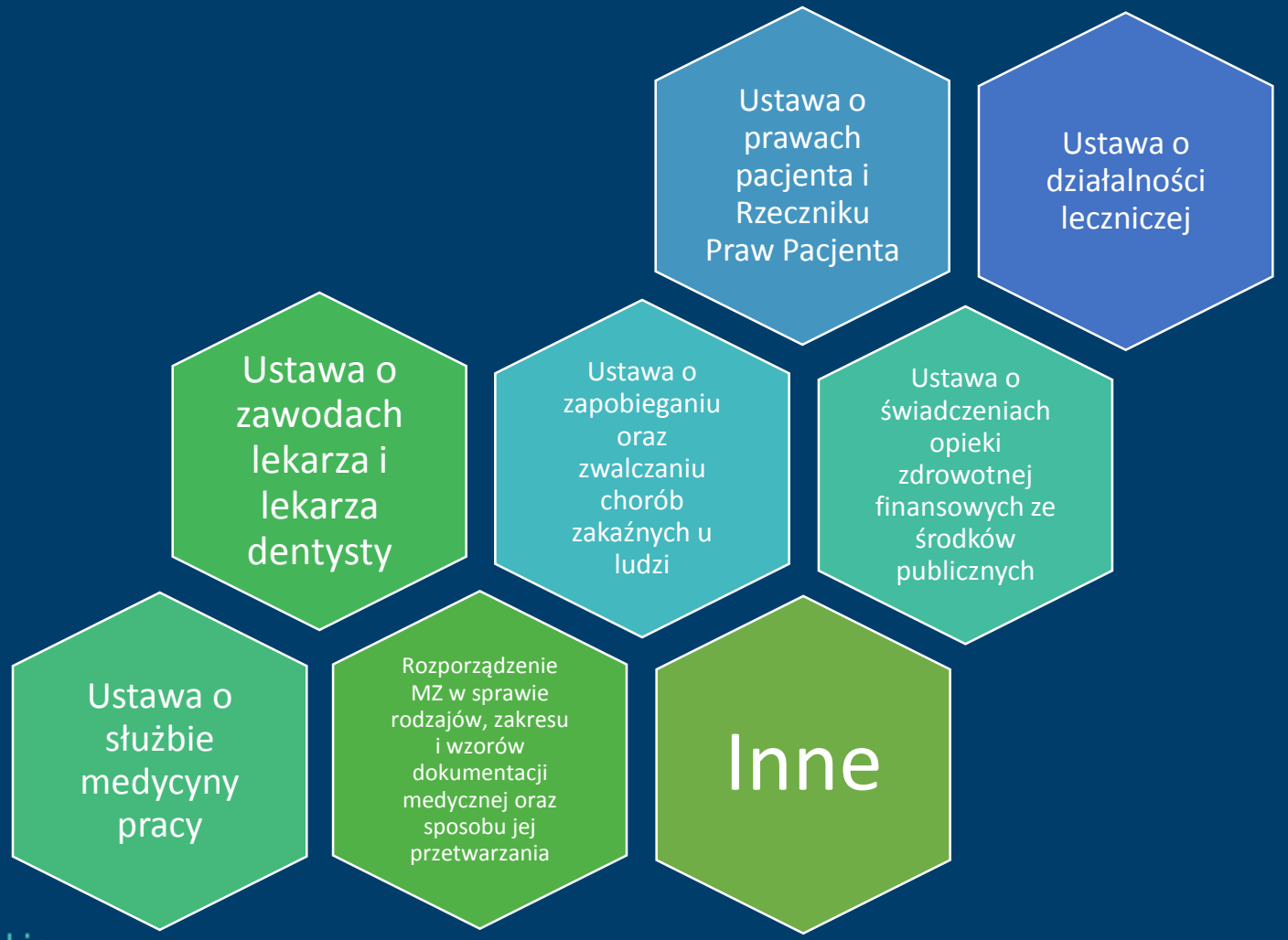
Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

Podstawy prawne przetwarzania w Polsce danych o stanie zdrowia



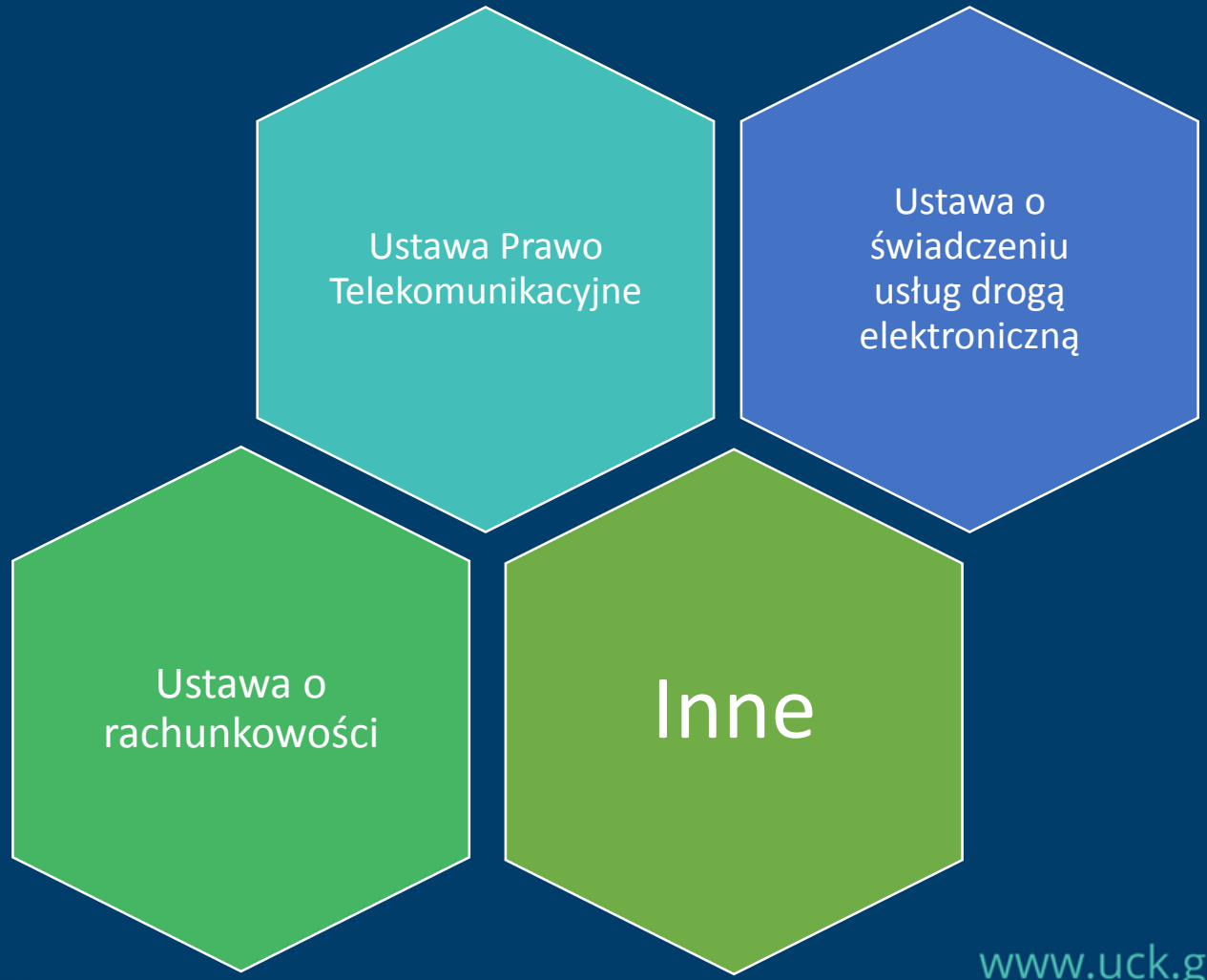
Przetwarzanie danych o stanie zdrowia: regulacje prawne

OBSZAR MEDYCZNY



Przetwarzanie danych o stanie zdrowia: regulacje prawne

INNE OBSZARY



Prawa osoby, których dane dotyczą

- Prawo do informacji i dostępu do danych: art. 13-15 RODO:
  - Art. 13 RODO – Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą
  - Art. 14 RODO – Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą
  - Art. 15 RODO – prawo dostępu do danych
- Prawo do sprostowania danych: art. 16 RODO
- Prawo do usunięcia danych (prawo do bycia zapomnianym): art. 17 RODO
- Prawo do ograniczenia przetwarzania: art. 18 RODO
- Prawo do przenoszenia danych: art. 20 RODO
- Prawo do sprzeciwu: art. 21 RODO

Obowiązki Administratora (art. 24 RODO)

Obowiązki Administratora:

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, ww. środki obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

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

Privacy by design (art. 25 ust. 1 RODO)

Uwzględnianie ochrony danych osobowych w fazie projektowania (privacy by design)

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

Zarządzanie ryzykiem, ocena skutków

Privacy by default (art. 25 ust. 2 RODO)

Domyśla ochrona danych (privacy by default)

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

Obowiązek ten odnosi się do:

- ilości zbieranych danych,
- zakresu ich przetwarzania,
- okresu ich przechowywania oraz
- ich dostępności.

W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Bezpieczeństwo przetwarzania (art. 32 RODO)

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

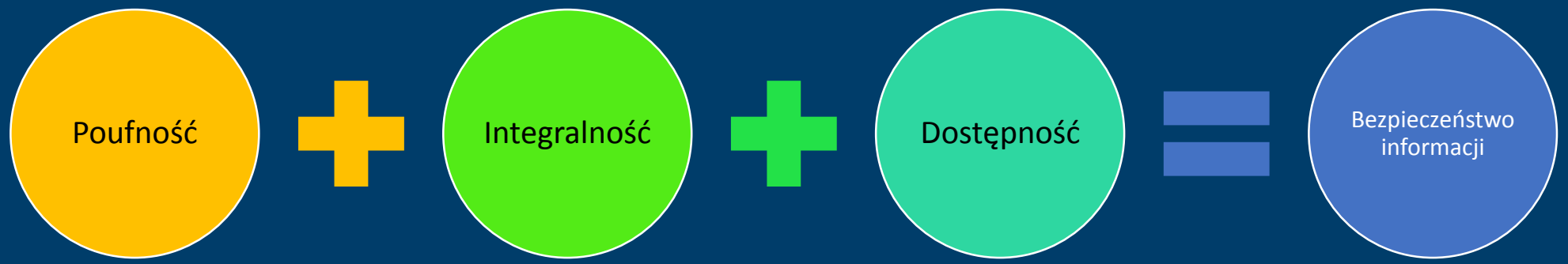
- pseudonimizację i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Bezpieczeństwo przetwarzania (art. 32 RODO)

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego

Bezpieczeństwo przetwarzania



Bezpieczeństwo przetwarzania

Szereg **obowiązków nałożonych na pracowników UCK** w procedurach Zintegrowanego Systemu Zarządzania (ZSZ), a zwłaszcza w **procedurach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)**

(PZ, PZ-ZI)

Naruszenie ODO (art. 4 pkt 12 RODO)

Art. 4 pkt 12 RODO

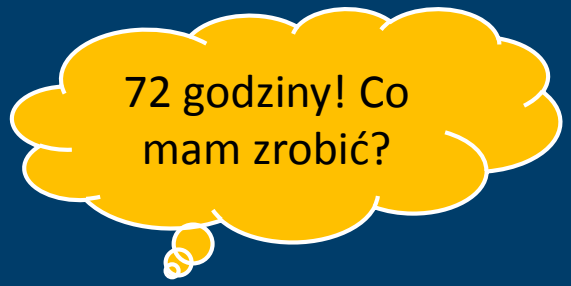
„Naruszenie ochrony danych osobowych” – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

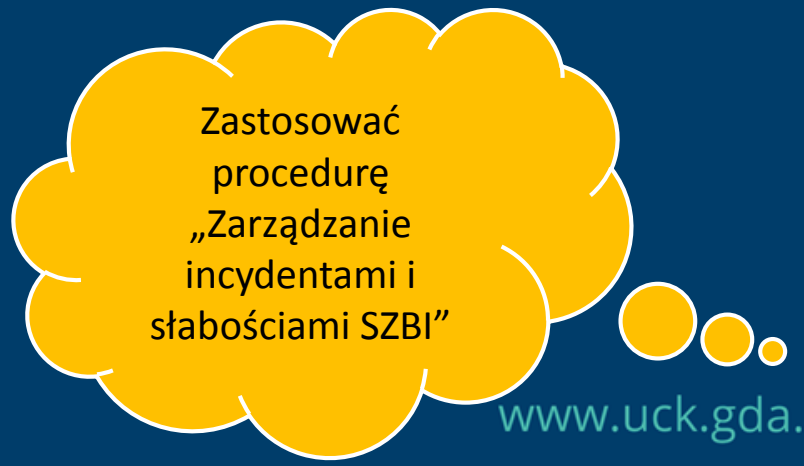
Zgłaszanie naruszeń Organowi Nadzorczemu

Art. 33 ust. 1 i 2 RODO

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.





Wyłączenie zgłoszenia naruszenia

Zawiadomienie o naruszeniu osoby, której dane dotyczą nie jest wymagane, jeśli:

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
- wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Powiadomienie o naruszeniu osoby, której dane dotyczą

Motyw 86 RODO

Administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych.
Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków.
Informacje należy przekazywać (…) tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania. Na przykład potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie.

Odpowiedzialność za naruszenia

Odpowiedzialność administracyjna

administracyjna kara pieniężna do 20 mln. EUR lub 4 % całkowitego rocznego obrotu przedsiębiorstwa – zastosowanie ma kara wyższa

UODO: podmioty publiczne – do 100 tys. zł.

Odpowiedzialność karna

Odpowiedzialność odszkodowawcza

Odpowiedzialność dyscyplinarna

Dziękuję za uwagę

Monika Golubska

Pełnomocnik Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji

Inspektor Ochrony Danych

mgolubska@uck.gda.pl
tel. 58 349 21 73