ISPOZ

Instytut
Specjaliści Prawa
Ochrony Zdrowia

RODO - jego konsekwencje dla placówek medycznych i lekarzy prowadzących praktyki indywidualne

Gdańsk, 24 marca 2018r.

Informacja o prawach autorskich

RODO

Rozporządzenie 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

ZAKRES ZASTOSOWANIA

bezpośrednio stosowane we wszystkich państwach członkowskich UE

bez potrzeby implementacji do polskiego porządku prawnego

weszło w życie z dniem 25 maja 2016r.,
w państwach członkowskich

będzie stosowane dopiero od 25 maja 2018r.

ZAKRES ZASTOSOWANIA

- **wszystkie podmioty** wykonujące działalność leczniczą > podmioty lecznicze praktyki i zawodowe

- **wszystkie dane osobowe** związane z prowadzeniem działalności gospodarczej > działalności leczniczej

nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze

PODSTAWOWE POJĘCIA

DANE OSOBOWE

wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej

osobę fizyczną można uznać za „zidentyfikowaną”,
jeśli w grupie osób można ją odróżnić od wszystkich pozostałych członków grupy

nie dotyczy danych osoby prawnej

DANE OSOBOWE

- numery identyfikacyjne
- cechy fizyczne lub fizjologiczne
- informacje majątkowe
- cechy nabyte

DANE OSOBOWE

- informacji **nie uważa się za umożliwiającą określenie** tożsamości, **jeżeli wymagałoby to nadmiernych kosztów, czasu i działań.**

- **danymi osobowymi nie są pojedyncze informacje o dużym stopniu ogólności**

DANE WRAŻLIWE

dane obejmujące:

1. pochodzenie rasowe lub etniczne / poglądy polityczne / przekonania religijne lub filozoficzne /

2. przynależność wyznaniową, partyjną lub związkową

3. dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych

4. **dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym**

DANE DOTYCZĄCE ZDROWIA

- **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

- **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;

DANE DOTYCZĄCE ZDROWIA

- informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych

- 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

DANE BIOMETRYCZNE

dane osobowe, które wynikają ze specjalnego przetwarzania technicznego

dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej

umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby

DANE ZWYKŁE

- **wszystkie pozostałe dane**, których nie można zaliczyć do kategorii danych wrażliwych

imię i nazwisko / data urodzenia / imiona rodziców / PESEL / adres zamieszkania

ZBIÓR DANYCH

- **uporządkowany zestaw danych osobowych** dostępnych według określonych kryteriów > niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

- dotychczasowy obowiązek rejestracji zbiorów danych zostanie całkowicie uchylony

- koniec obowiązywania rozporządzenia Min. Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych

PRZETWARZANIE DANYCH

wszelkie operacje wykonywane na danych osobowych

zbieranie / utrwalanie / wykorzystanie /
przechowywanie / opracowywanie /
zmienianie / łączenie / zestawianie /
udostępnianie / rozpowszechnianie /
przesyłanie / usuwanie

PRZETWARZANIE DANYCH WRAŻLIWYCH

art. 9 RODO

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 fizycznej lub **danych dotyczących zdrowia,** seksualności lub orientacji seksualnej tej osoby

DANE WRAŻLIWE
A UDZIELANIE ŚWIADCZEŃ ZDROWOTNYCH

przetwarzanie danych o zdrowiu
dopuszczalne wyjątkowo gdy:

- jest niezbędne do 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

instytucje ochrony danych osobowych

ADO / IODO / PUODO / RPP

ADMINISTRATOR DANYCH (ADO)

ten kto ustala cele przetwarzania i sposoby przetwarzania danych

osoba fizyczna / osoba prawna / organ publiczny / jednostka lub inny podmiot

OBOWIĄZKI ADO

- przetwarzanie zgodnie z prawem

- zbieranie dla oznaczonych, zgodnych z prawem celów

- środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych

- zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym

- ułatwia osobie, której dane dotyczą, wykonanie przysługujących jej praw

ROZLICZALNOŚĆ

administrator jest odpowiedzialny za przestrzeganie przepisów
zasad przetwarzania

administrator musi być w stanie wykazać ich przestrzeganie

EWIDENCJA OSÓB UPOWAŻNIONYCH

prowadzi ADO/ABI

1. **imię i nazwisko osoby upoważnionej**
2. **data nadania i ustania upoważnienia**
3. **zakres upoważnienia do przetwarzania danych osobowych**
4. **identyfikator**

jeżeli dane są przetwarzane w systemie informatycznym

POWOŁANIE IODO

Inspektor Ochrony Danych Osobowych (IODO) – zastępuje dotychczasowego ABI

powołanie IODO to decyzja ADO

fakultatywne / obligatoryjne

KWALIFIKACJE IODO

brak szczególnych wymogów kwalifikacyjnych

wymagana wiedza i praktyka w zakresie zasad przetwarzania danych osobowych

+

umiejętność wypełnienia zadań

AUTONOMIA / STATUS IODO

ma być właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych

osoby, których dane dotyczą, mogą kontaktować się z IODO we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących

status IODO

ZADANIA IODO

• **informowanie administratora / pracowników,** którzy przetwarzają dane osobowe, **o obowiązkach wynikających z przepisów prawa**

• **doradzanie** w sprawie ochrony danych osobowych

• **monitorowanie przestrzegania przepisów oraz polityk administratora w dziedzinie ochrony danych osobowych,**

• **współpraca z Prezesem Urzędu**

ZGŁOSZENIE IODO

(projekt ustawy)

- **zawiadomienia Prezesa Urzędu o wyznaczeniu IODO** > termin, forma

- **zawiadomienie o każdej zmianie danych**

- **opublikowanie danych kontaktowych IODO** przez administratora

Prezes Urzędu Ochrony Danych Osobowych (PUODO)

(projekt ustawy)

organ nadzorczy w rozumieniu RODO

zastąpi Generalnego Inspektora Ochrony Danych Osobowych (GIODO)

będzie udostępniał w BIP

1. standardowe klauzule umowne
2. zatwierdzone kodeksy postępowania

kontrola PUODO

(projekt ustawy)

- zawiadomienie o zamiarze kontroli

projekt a regulacja u.s.d.g.

kontrola przeprowadzana **na podstawie przepisów ustawy o swobodzie działalności gospodarczej**

z wyłączeniem niektórych przepisów

czynności sprawdzające na podstawie pisemnego upoważnienia Prezesa Urzędu

uprawnienia kontrolerów

(projekt ustawy)

1. **wstęp w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń**

2. **wgląd do wszelkich dokumentów** i wszelkich informacji mających bezpośredni związek z przedmiotem kontroli

3. **przeprowadzanie oględzin** miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych

4. **żądanie złożenia pisemnych lub ustnych wyjaśnień** oraz **przesłuchiwać w charakterze świadka** osoby w zakresie niezbędnym do ustalenia stanu faktycznego

5. **zlecanie sporządzenia ekspertyz i opinii**

przebieg kontroli

(projekt ustawy)

w obecności administratora / osoby upoważnionej

jeżeli nie ma przedst. administratora / os. upoważnionej **może być osoba pozostająca w lokalu przedsiębiorcy / przywołany świadek**

kontrolujący **może przesłuchać pracownika** kontrolowanego **w charakterze świadka**

jeżeli mimo prawidłowego wezwania świadek nie stawił się bez uzasadnionej przyczyny / bezzasadnie odmówił złożenia zeznań **może być ukarany karą grzywny do 5 000 zł**

przebieg kontroli

(projekt ustawy)

kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli **warunki i środki** niezbędne do sprawnego przeprowadzenia kontroli

obowiązek sporządzenia we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach

kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków

w wypadku odmowy potwierdza kontroler

skutek kontroli

(projekt ustawy)

1. niestwierdzenie naruszeń > **brak dalszych czynności**

2. mogło dojść do naruszenia przepisów o ochronie danych osobowych > **wszczęcie postępowania przez Prezesa Urzędu**

3. Prezes Urzędu **może żądać wszczęcia postępowania dyscyplinarnego** lub innego przewidzianego prawem postępowania **przeciwko osobom winnym uchybień**

4. w razie stwierdzenia, że działanie lub zaniechanie wyczerpuje znamiona przestępstwa > **Prezes Urzędu kieruje zawiadomienie o popełnieniu przestępstwa**

postępowanie
w przedmiocie naruszenia przepisów
(projekt ustawy)

może być zainicjowane przez:

1. **osobę, której danych dotyczy naruszenie**

2. organizację społeczną
do której zadań należą sprawy
związane z ochroną danych osobowych

3. **z urzędu**

postępowanie
w przedmiocie naruszenia przepisów
(projekt ustawy)

jeżeli liczba stron przekracza 20 osób możliwe zawiadomienie stron o decyzjach i innych czynnościach **w formie publicznego obwieszczenia** / w innej formie publicznego ogłoszenia zwyczajowo przyjętej w danej miejscowości / przez udostępnienie pisma w BIP

nieusprawiedliwione niestawiennictwo na przesłuchanie – **PUODO może nałożyć karę grzywny** od 500 zł do 5000 zł

tymczasowe ograniczenie przetwarzania
(projekt ustawy)

- **PUODO może zobowiązać podmiot**
do ograniczenia przetwarzania danych
w toku postępowania

- **jeżeli dalsze przetwarzanie mogłoby spowodować poważne i trudne do usunięcia skutki**

- **w drodze postanowienia (zaskarżalne)**

- **określony czas obowiązywania**
nie dłużej niż do czasu wydania decyzji

rozstrzygnięcia PUODO

1. **upomnienie** w przypadku naruszenia przepisów RODO
2. **ostrzeżenie** dot. możliwości naruszenia przepisów przez planowane operacje
3. **nakazanie spełnienia żądania** osoby, której dane dotyczą
4. **nakazanie dostosowania operacji przetwarzania** do przepisów RODO > wskazanie sposobu i terminu
5. **nakazanie zawiadomienia osoby**, której dane dotyczą, **o naruszeniu ochrony danych**
6. **wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania**, w tym zakazu przetwarzania
7. **nakazanie sprostowania / usunięcia danych osobowych**
8. **cofnięcie certyfikacji**
9. **administracyjna kara pieniężna**
10. **nakazanie zawieszenia przepływu danych** do odbiorcy w państwie trzecim

ADMINISTRACYJNA KARA PIENIĘŻNA

- nakładana w drodze decyzji

- **wyjątek od natychmiastowej wykonalności kary**
  ale i tak będą dość szybko egzekwowane

- **płatna w terminie 14 dni**
  od uprawomocnienia orzeczenia sądu administracyjnego

- podlega ściągnięciu
  w drodze postępowania egzekucyjnego w administracji

ADMINISTRACYJNA KARA PIENIĘŻNA

do 10 000 000 EURO

- **niewłaściwe zabezpieczenie danych**
- **niezgłoszenie naruszeń ochrony danych lub niezawiadomienie o naruszeniu**
- **nieopublikowanie danych inspektora ochrony danych**
- naruszenie wymogów certyfikacyjnych
- naruszenie zasad zgody przy świadczeniu usług drogą elektroniczną

ADMINISTRACYJNA KARA PIENIĘŻNA

do 20 000 000 EURO

- **naruszenie podstawowych zasad przetwarzania**
- **niewypełnienie obowiązku informacyjnego**
- **nieuzasadniona odmowa sprostowania / usunięcia**
- niewłaściwe uzyskanie zgody
- przetwarzanie bez zgody

ZASADY WYMIARU KARY

a. **charakter waga i czas trwania naruszenia**
przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania / liczby poszkodowanych osób, których dane dotyczą / rozmiaru poniesionej przez nie szkody

b. **umyślny lub nieumyślny charakter naruszenia**

c. **działania podjęte przez administratora** lub podmiot przetwarzający **w celu zminimalizowania szkody** poniesionej przez osoby, których dane dotyczą

d. **stopień odpowiedzialności administratora** lub podmiotu przetwarzającego **z uwzględnieniem środków technicznych i organizacyjnych wdrożonych**

ZASADY WYMIARU KARY

e. **wszelkie stosowne wcześniejsze naruszenia** ze strony administratora lub podmiotu przetwarzającego

f. stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków

g. kategorie danych osobowych, których dotyczyło naruszenie

h. sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie

CERTYFIKATY

- **możliwość wystąpienia do Prezesa UODO /** instytucji akredytowanej o wydanie certyfikatu w zakresie ochrony danych osobowych

- **mają świadczyć o zgodności przetwarzania danych z RODO** przez administratorów / podmioty przetwarzające

- na wniosek zainteresowanego podmiotu

- **rejestr podmiotów które uzyskały certyfikaty**

CERTYFIKATY

- otrzymanie certyfikatu **nie zwolni z obowiązku przestrzegania przepisów**

- kryteria certyfikacyjne będzie publikował Prezes UODO w BIP
proces uzyskiwania ma być przejrzysty

- na razie nie przewiduje się premiowania placówek posiadających taki certyfikat
np. w ramach kryteriów oceny ofert

AKREDYTACJA

- **Polskie Centrum Akredytacji** będzie udzielać akredytacji do udzielania certyfikacji

- kryteria akredytacyjne będą publikowane w BIP

- **podmioty certyfikujące przedstawiają** Prezesowi UODO **powody udzielenia lub cofnięcia żądanej certyfikacji**

KODEKSY BRANŻOWE

zrzeszenia i podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające **z poszczególnych sektorów** mogą opracowywać i wdrażać wspólne kodeksy postępowania

próby tworzenia kodeksu postępowania dla sektora ochrony zdrowia
(tylko dla podmiotów leczniczych)

- **Prezes UODO będzie zatwierdzał dany kodeks branżowy > publikacja w BIP**

KODEKSY BRANŻOWE

dobrowolność przyjmowania do stosowania kodeksów

stosowanie zatwierdzonych kodeksów postępowania może być wykorzystane jako element ułatwiający i umożliwiający wykazanie przez administratora wypełniania ciążących na nim obowiązków

- **możliwość zmiany lub rozszerzenia zakresu „obowiązujących” kodeksów**

RZECZNIK PRAW PACJENTA

UPRAWNIENIA RPP

prowadzenie postępowań w sprawach praktyk naruszających zbiorowe prawa pacjentów

prowadzenie postępowań w zakresie naruszenia praw pacjenta

możliwość wszczęcia i uczestniczenia w sprawach cywilnych dotyczących naruszenia praw pacjenta

analiza skarg pacjentów w celu określenia zagrożeń i obszarów w systemie ochrony zdrowia wymagających naprawy

WSZCZĘCIE POSTĘPOWANIA WYJAŚNIAJĄCEGO

jeżeli poweźmie wiadomość co najmniej uprawdopodabniającą naruszenie praw pacjenta

z urzędu / na wniosek osoby zainteresowanej

Rzecznik może odmówić ujawnienia nazwiska i innych danych osobowych pacjenta, który złożył skargę / którego skarga dotyczy, jeżeli uzna to za niezbędne dla ochrony praw tego pacjenta

SKARGA DO RPP

w odpowiedzi na skargę RPP może:

1. **podjąć sprawę** (wszcząć postępowanie)

2. **poprzestać na wskazaniu** wnioskodawcy przysługujących mu / pacjentowi **środków prawnych**

3. **przekazać sprawę** według właściwości

4. **nie podjąć sprawy**

POSTĘPOWANIE PRZED RPP

może zbadać, nawet bez uprzedzenia, każdą sprawę na miejscu

może żądać złożenia wyjaśnień

może skierować wystąpienie do organu, organizacji lub instytucji, **w których działalności stwierdził naruszenie** praw pacjenta

może zwrócić się do organu nadrzędnego z wnioskiem o zastosowanie środków przewidzianych w przepisach prawa

WYSTĄPIENIE RPP

w wystąpieniu do podmiotu Rzecznik formułuje opinie lub wnioski co do sposobu załatwiania sprawy, a także może żądać wszczęcia postępowania dyscyplinarnego lub zastosowania sankcji służbowych

w terminie 30 dni podmiot może poinformować Rzecznika o podjętych działaniach lub zajętym stanowisku

PODSTAWY PRAWNE PRZETWARZANIA DANYCH W OCHRONIE ZDROWIA

ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

w ochronie zdrowia przetwarzanie danych

jest niezbędne do wypełnienia obowiązku

prawnego ciążącego na administratorze

ZAKRES - PODSTAWY PRAWNE

ustawa z dnia 27 sierpnia 2004r.

o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych

(t.j., Dz.U. z 2015r., poz. 581 z późn. zm.)

ustawa z dnia 6 listopada 2008r.

o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j., Dz.U. z 2017r., poz. 1318 z późn. zm.)

ZAKRES - PODSTAWY PRAWNE

Rozporządzenie Ministra Zdrowia
w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania
z dnia 9 listopada 2015 r.

Rozporządzenie Ministra Zdrowia
w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców,
szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych
z dnia 20 czerwca 2008 r.

DANE W DOKUMENTACJI MEDYCZNEJ

oznaczenie pacjenta

(art. 25 pkt 1 ustawy o prawach pacjenta)

a. nazwisko i imię (imiona),

b. datę urodzenia,

c. oznaczenie płci,

d. adres miejsca zamieszkania,

e. numer PESEL, jeżeli został nadany, w przypadku noworodka - numer PESEL matki, a w przypadku osób, które nie mają nadanego numeru PESEL - rodzaj i numer dokumentu potwierdzającego tożsamość,

f. w przypadku gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody - nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania;

DANE W DOKUMENTACJI MEDYCZNEJ

informacje dotyczące stanu zdrowia lub udzielonych pacjentowi świadczeń
(art. 25 pkt 1 ustawy o prawach pacjenta)

informacje dotyczące stanu zdrowia i choroby oraz procesu diagnostycznego, leczniczego, pielęgnacyjnego lub rehabilitacji
(§ 10 ust 5. rozp. dokum. med.) w szczególności:

opis udzielonych świadczeń zdrowotnych / rozpoznanie choroby, problemu zdrowotnego, urazu lub rozpoznanie ciąży / zalecenia / informacje o wydanych orzeczeniach, opiniach lekarskich lub zaświadczeniach / informacje o lekach, wraz z dawkowaniem, lub wyrobach medycznych przepisanych pacjentowi na receptach lub zleceniach na zaopatrzenie w wyroby medyczne

DANE W CELACH ROZLICZENIOWYCH

dane charakteryzujące osobę, której udzielono świadczenia

a) **identyfikator osoby (PESEL) oraz kod identyfikatora**;
identyfikatorem dziecka, któremu nie został nadany numer PESEL, jest identyfikator jednego z rodziców lub identyfikator opiekuna prawnego dziecka

b) **unikalny numer identyfikacyjny karty onkologicznej** -
w przypadku osoby, której wydano kartę onkologiczną, oraz w przypadku gdy diagnostyka onkologiczna lub leczenie onkologiczne są udzielane na podstawie karty onkologicznej

c) **imię (imiona) i nazwisko**

DANE W CELACH ROZLICZENIOWYCH

adres miejsca zamieszkania pacjenta
a jeżeli osoba, której udzielono świadczenia, nie ma miejsca zamieszkania na terytorium RP także adres miejsca pobytu na terytorium Rzeczypospolitej Polskiej, na który składają się: państwo / nazwa miejscowości / kod pocztowy / ulica, numer domu i lokalu / nazwa: gminy, powiatu i województwa

numer telefonu kontaktowego
lub adres poczty elektronicznej pacjenta
- jeżeli został wskazany

datę urodzenia pacjenta / płeć pacjenta

DANE W CELACH ROZLICZENIOWYCH

kod tytułu uprawnienia do świadczeń

dane identyfikujące dokument
w przypadku potwierdzenia prawa do świadczeń opieki zdrowotnej kod tytułu uprawnienia dodatkowego

nazwę dokumentu,
który potwierdza uprawnienia dodatkowe
oraz dane identyfikujące ten dokument

dane przedstawiciela ustawowego
albo opiekuna faktycznego (imię / imiona i nazwisko, adres miejsca zamieszkania

ZGODA NA PRZETWARZANIE

dobrowolne > konkretne > świadome > jednoznaczne

okazanie woli

pisemna?

wyraźne działanie potwierdzające

osoba w pełni władz umysłowych / bez przymusu

ZGODA NA PRZETWARZANIE

osoba, której dane dotyczą, **powinna znać przynajmniej tożsamość administratora** oraz zamierzone cele przetwarzania danych osobowych

w zrozumiałej i łatwo dostępnej formie jasnym i prostym językiem

jeżeli w jednym dokumencie - zapytanie o zgodę musi zostać przedstawione **w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii**

COFNIĘCIE ZGODY

-skutek cofnięcia zgody:

-co do przeszłości

-co do przyszłości

- czy można pozbawić możliwości cofnięcia zgody?

PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

na gruncie RODO

Prawo do uzyskania informacji przed wyrażeniem zgody na przetwarzanie

Prawo dostępu do danych

Prawo do sprostowania danych

Prawo do usunięcia danych „prawo do bycia zapomnianym”

Prawo do ograniczenia przetwarzania

Prawo do przenoszenia danych

OBOWIĄZEK INFORMACYJNY

(„przed zbieraniem danych”) projekt ustawy

a) tożsamość i dane kontaktowe administratora

b) dane kontaktowe inspektora ochrony danych

c) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania

d) kategorie danych osobowych

e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją

f) informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim

OBOWIĄZEK INFORMACYJNY

projekt ustawy z 8 lutego 2018r.

informacje o prawie:

1. **dostępu do danych osobowych**
2. **sprostowania danych**
3. *usunięcia danych*
4. **ograniczenia przetwarzania**
5. *o prawie do wniesienia sprzeciwu wobec przetwarzania*
6. *o prawie do przenoszenia danych*

OBOWIĄZEK INFORMACYJNY

projekt ustawy z 8 lutego 2018r.

- **Obowiązek informacyjny przed zbieraniem danych**

- **Obowiązek informacyjny „na żądanie” / prawo dostępu do danych „na żądanie”**

- **Rozszerzony obowiązek informacyjny**

PRAWO DOSTĘPU DO DANYCH (RODO)

prawo do potwierdzenia, że dane są przetwarzane przez administratora

obowiązek dostarczenia kopii danych przetwarzanych > opłata

formy wniosku

PRAWO DO SPROSTOWANIA (RODO)

prawo żądania niezwłocznego sprostowania

prawo żądania uzupełnienia

obowiązek zawiadomienia > termin / możliwość przedłużenia

POWIERZENIE PRZETWARZANIA DANYCH

nowe wymogi dla umów z podmiotami zewnętrznymi

PODMIOT PRZETWARZAJĄCY

- forma organizacyjna

-w imieniu ADO

-wyjątkowo obowiązek prawny

POWIERZENIE PRZETWARZANIA DANYCH

-
- **może dotyczyć całości lub części danych**
- powierzenie danych innemu podmiotowi **wymaga zawarcia umowy > forma**

POWIERZENIE PRZETWARZANIA DANYCH

korzystanie **wyłącznie z usług takich podmiotów, które zapewniają wystarczające gwarancje** wdrożenia odpowiednich środków technicznych i organizacyjnych,

POWIERZENIE PRZETWARZANIA DANYCH

- usługi dalszego podmiotu przetwarzającego > warunki

- informacja o zmianach > reakcja administratora

TREŚĆ UMOWY

podmiot przetwarzający

1. **przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora**

2. **zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy** lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy

3. **w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne** wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw

TREŚĆ UMOWY

podmiot przetwarzający

4. **pomaga administratorowi wywiązać się z obowiązków**

5. **po zakończeniu świadczenia usług** związanych z przetwarzaniem **zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe** oraz usuwa wszelkie ich istniejące kopie

6. **udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków**

7. **umożliwia administratorowi** lub audytorowi upoważnionemu przez administratora **przeprowadzanie audytów**

ŚRODKI OCHRONY DANYCH

techniczne, organizacyjne

ŚRODKI BEZPIECZEŃSTWA (RODO)

regulacja RODO nie odbiega co do zasady istotnie od dotychczasowych rozwiązań prawnych

samodzielna ocena administratora i podmiotu przetwarzającego przez pryzmat ryzyka i możliwości

> określenie odpowiedniego poziomu oraz metod stosowanych zabezpieczeń

ŚRODKI BEZPIECZEŃSTWA (RODO)

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych […] utraci moc obowiązującą po wejściu RODO

- **rekomendacje w BIP**

- **większa odpowiedzialność administratorów i inspektorów**

ŚRODKI BEZPIECZEŃSTWA (RODO)

NALEŻY UWZGLĘDNIĆ:

- stan wiedzy technicznej i koszt wdrażania
- charakter, zakres, kontekst i cele przetwarzania
- ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia

PRZYKŁADOWE ŚRODKI BEZPIECZEŃSTWA (RODO)

- pseudonimizacja / 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

- audyt bezpieczeństwa

PSEUDONIMIZACJA

przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, **bez użycia dodatkowych informacji,**

warunki przechowywania danych

SZYFROWANIE

nie jest pojęciem zdefiniowanym w RODO

brak wskazówek co do szczegółów i wymagań procesu szyfrowania

nie prowadzi do pozbawienia informacji cech osobowych

DOKUMENTY TOŻSAMOŚCI

eWUŚ

„świadczeniobiorca **potwierdzi swoją tożsamość poprzez okazanie** dowodu osobistego, paszportu, prawa jazdy albo legitymacji szkolnej; legitymacja szkolna może być okazana jedynie przez osobę, która nie ukończyła 18. roku życia”

inny dokument / oświadczenie

„świadczeniobiorca **po okazaniu dokumentu**, o którym mowa w ust. 2 pkt 1, może przedstawić inny dokument potwierdzający prawo do świadczeń,
a jeżeli takiego dokumentu nie posiada, złożyć pisemne oświadczenie o przysługującym mu prawie do świadczeń opieki zdrowotnej”

REJESTRACJA PACJENTÓW

- zasady weryfikacji osób dzwoniących

- zasady weryfikacji osób rejestrujących się osobiście

UDOSTĘPNIANIE DOKUMENTACJI

- **na zasadach określonych w ustawie**
o prawach pacjenta i Rzeczniku Praw Pacjenta

SPOSOBY UDOSTĘPNIANIA DOKUMENTACJI

1. **do wglądu**
2. **sporządzenie wyciągu / odpisu / kopii / wydruku**
3. **wydanie oryginału**
   za potwierdzeniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu
4. **środki komunikacji elektronicznej**
5. **informatyczne nośniki danych**

DOKUMENTACJA RODO

DOKUMENTACJA (RODO)

cele administratora > zgodność z RODO

środki techniczne i organizacyjne

rozliczalność

REJESTR CZYNNOŚCI PRZETWARZANIA

1. **imię i nazwisko lub nazwę** oraz dane kontaktowe **administratora**, a także przedstawiciela administratora oraz **inspektora ochrony danych**

2. **cele przetwarzania**

3. **opis kategorii osób, których dane dotyczą** oraz kategorii danych osobowych

4. **kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione** w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych

REJESTR CZYNNOŚCI PRZETWARZANIA

5. **jeżeli przekazania danych osobowych do państwa trzeciego** lub organizacji międzynarodowej
dokumentacja odpowiednich zabezpieczeń

6. jeżeli jest to możliwe, **planowane terminy usunięcia** poszczególnych kategorii **danych**

7. **ogólny opis** technicznych i organizacyjnych **środków bezpieczeństwa**

DOKUMENT OCENY SKUTKÓW DLA OCHRONY DANYCH

administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych
> **konsultuje się z IODO**

fakultatywny czy obligatoryjny?

DOKUMENT OCENY SKUTKÓW DLA OCHRONY DANYCH

minimalna zawartość:

1. **systematyczny opis planowanych operacji przetwarzania**
   i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora

2. **ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne** *w stosunku do celów*

3. **ocenę ryzyka naruszenia praw**
   lub wolności osób, których dane dotyczą

4. **środki planowane w celu zaradzenia ryzyku**
   w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy

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

OBOWIĄZEK ZGŁASZANIA NARUSZEŃ

- obowiązek administratora
- termin
- forma
- opóźnienie > wyjaśnienia
- brak obowiązku > kiedy
- sukcesywna informacja
- treść zgłoszenia

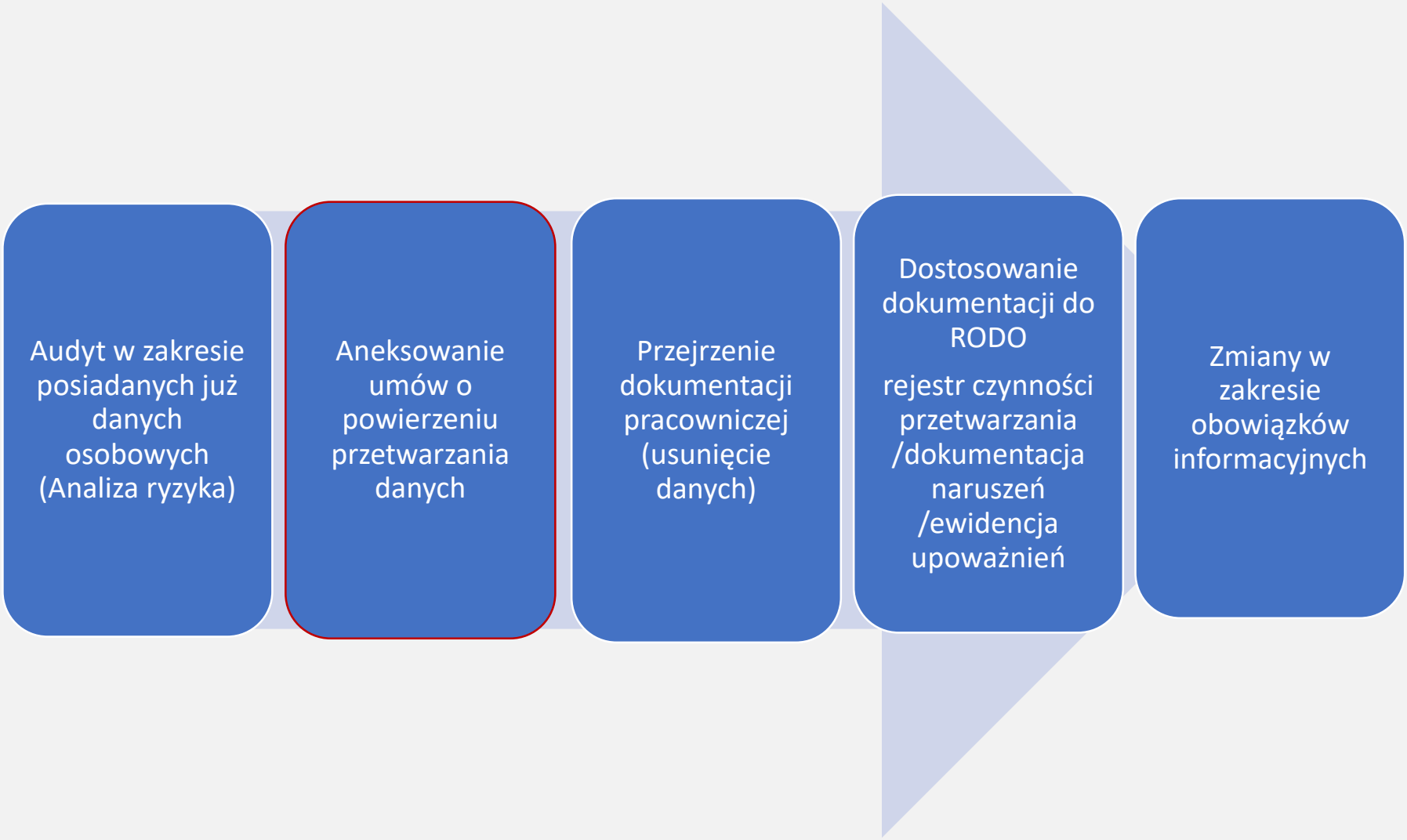
ZAWIADOMIANIE OSOBY O NARUSZENIACH

- **obowiązek administratora**
- **język i forma**
- **minimalna zawartość zawiadomienia**
- **wyłączenia**

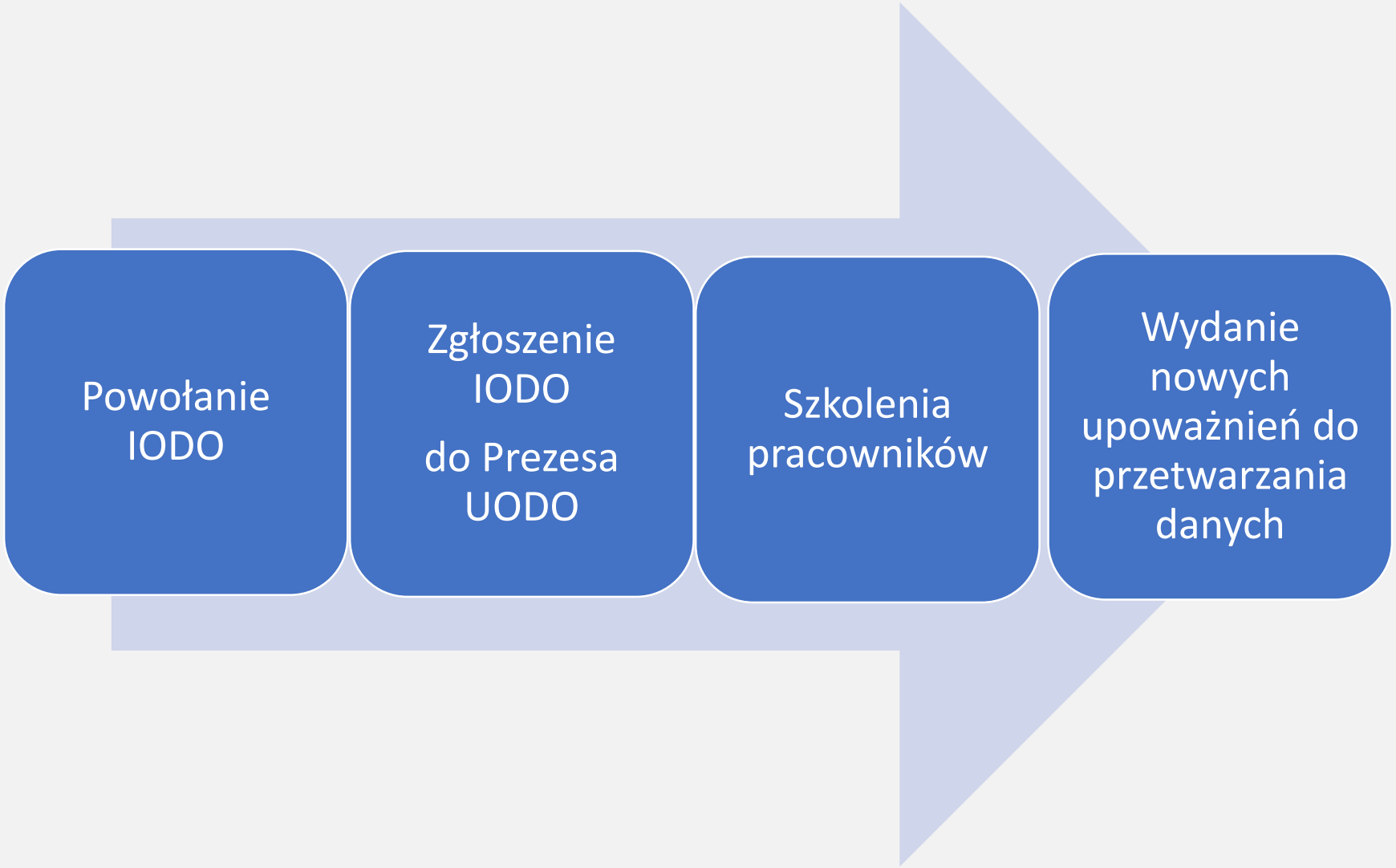
DOKUMENTACJA NARUSZEŃ

- **okoliczności naruszenia** ochrony danych osobowych
- **skutki naruszenia**
- **podjęte działania zaradcze**
- **procedura na wypadek naruszenia bezpieczeństwa**

SCHEMAT WPROWADZANIA RODO



SCHEMAT WPROWADZANIA RODO



Informacja o prawach autorskich

ISPOZ

Instytut
Specjaliści Prawa
Ochrony Zdrowia

DZIĘKUJEMY

ZA UWAGĘ

Gdańsk, 24 marca 2018r.