Nazwa szkolenia:

WDRAZANIE RODO W PRAKTYKACH ZAWODWYCH LEKARZY I LEKARZY DENTYSTÓW

Termin: 16.06.2018

Trener:

radca prawny Katarzyna Godlewska

AKTY PRAWNE - docelowo

- 1. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. o ochronie danych **PRAWO INTELIGENTNE**
- 2. ustawa o ochronie danych osobowych z 10 maja 2018 r. (Dz.U.z 2018 r. poz. 1000)
- 3. kodeksy branżowe:

  kodeks postępowania dla podmiotów sektora ochrony zdrowia dotyczący ochrony danych osobowych

Ministerstwo Cyfryzacji-projekt ustawy o ochronie danych osobowych

Rozporządzenie jest co do zasady bezpośrednio skutecznym aktem prawa unijnego, jednak wymaga w niektórych przypadkach podjęcia krajowych działań legislacyjnych. Założeniem przyświecającym tworzeniu takich przepisów prawnych ma być pełne poszanowanie prawa unijnego. Działania podejmowane przez Ministerstwo Cyfryzacji ograniczają się więc do tworzenia regulacji, do której podjęcia wprost upoważniają przepisy ogólnego rozporządzenia, bądź gdy jest to konieczne do zapewnienia jego skutecznego stosowania w polskiej przestrzeni prawnej.

USTAWA O PRAWACH PACJENTA I RZECZNIKU PRAW PACJENTA

- Art. 23. [Prawo do dostępu do dokumentacji medycznej]
- 1. Pacjent ma prawo do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych.
- 2. Dane zawarte w dokumentacji medycznej podlegają ochronie określonej w niniejszej ustawie oraz w przepisach odrębnych.

USTAWA O PRAWACH PACJENTA I RZECZNIKU PRAW PACJENTA

- Art. 13. *Pacjent* ma *prawo* do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego.

USTAWA O PRAWACH PACJENTA I RZECZNIKU PRAW PACJENTA

- Art. 14
- osoby wykonujące zawód medyczny są obowiązane zachować w tajemnicy informacje związane z *pacjentem*, w szczególności ze stanem zdrowia *pacjenta*.

ROZPORZĄDZENIE-Pojęcia

- „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;

ROZPORZĄDZENIE-Pojęcia

- „przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

DANE SENSYTYWNE

- „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 biometryczne” 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;
- „dane dotyczące zdrowia” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
- ***INFORMACJE O NAŁOGACH I UZALEŻNIENIACH – NALEŻA DO D.Z.***

ROZPORZĄDZENIE-Pojęcia

- **(35)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, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE [9)]; 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.

ROZPORZĄDZENIE-Pojęcia

(51) DANE DOTYCZĄCE ZDROWIA

- Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności. (…)…….MOTYW 53 …

DANE DOTYCZĄCE ZDROWIA

Art. 9 Rozporządzenia:

- Zakaz przetwarzania szczególnych kategorii danych osobowych, w tym danych dotyczących zdrowia (dane sensytywne)
- Zakaz nie jest bezwzględny- **WYJĄTKI-katalog zamknięty**

DANE SENSYTYWNE

Art. 9 UST.1 Rozporządzenia:

- 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 SENSYTYWNE-WYJĄTKI

Zakaz nie ma zastosowania, gdy spełniony jest jeden z poniższych warunków:

- **a)** osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
- **b)** przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
- **c)** przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

DANE SENSYTYWNE-WYJĄTKI

WYJATKI C.D.

h) przetwarzanie 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, o których mowa w ust. 3;

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; NP. ZAGROŻENIA EPIDEMICZNE

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

DANE SENSYTYWNE-WYJĄTKI

WYJATKI C.D.

Ust. 3 Dane osobowe sensytywne, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), 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.

Uprawnienie do przetwarzania danych wrażliwych na podstawie komentowanego przepisu obejmuje więc lekarzy, lekarzy dentystów, pielęgniarki, położne, fizjoterapeutów oraz diagnostów laboratoryjnych, jako że wszystkie te grupy zawodowe zobowiązane są do zachowania tajemnicy związanej z wykonywaniem swojego zawodu.

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

DANE SENSYTYWNE-WYJĄTKI

WYJATKI C.D.

Ust. 3 Dane osobowe sensytywne, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), 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.

„na odpowiedzialność pracownika podlegającego obowiązkowi zachowania tajemnicy" oznacza, że do przetwarzania takich danych może zostać dopuszczony każdy, pod warunkiem zawarcia odpowiedniej umowy, na mocy której odpowiedzialność za działania takiej osoby będzie ponosiła osoba związana obowiązkiem zachowania tajemnicy zawodowej np. sekretarka medyczna.

CO Z TĄ ZGODĄ?

"zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

CO Z TĄ ZGODĄ?

- Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
- Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.

CO Z TĄ ZGODĄ?

- Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
- Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

ZASADY PRZETWARZANIA DANYCH

Dane osobowe muszą być:

- **a)** przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („ZASADA zgodności z prawem, rzetelność i przejrzystość”);

- **b)** zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ZASADA ograniczenia celu”);

- **c)** adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („ZASADA minimalizacja danych”);

- **d)** prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („ZASADA prawidłowości”);

ZASADY PRZETWARZANIA DANYCH

Dane osobowe muszą być:

- **e)** przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ZASADA ograniczenia przechowywania”);
- **f)** przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („ZASADA integralności i poufności”).

ZASADY PRZETWARZANIA DANYCH

ZASADA ROZLICZALNOŚCI

Administrator jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

ROZPORZĄDZENIE-Pojęcia

- ADMINISTRATOR DANYCH
- PODMIOT PRZETWARZAJĄCY

ROZPORZĄDZENIE-Pojęcia

- „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; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
- Administratorem danych będzie m.in. Podmiot leczniczy- spółka reprezentowana przez zarząd, szpital jako spzoz, osoba fizyczna prowadząca działalność leczniczą.

POWIERZENIE DANYCH- PROCESOR

- Wielokrotnie w działalności *podmiotów leczniczych mamy do czynienia z tzw. „outsourcingiem”* wybranych obszarów działalności;
- Przy realizacji tych umów, porozumień, zamówień zobowiązujących lub umożliwiających zleceniobiorcom, wykonawcom dostęp do informacji zawierających dane osobowe. W takim przypadku mówimy o **powierzaniu danych osobowych do przetwarzania.**
- **PRZYKŁADY- biuro rachunkowe, firma Informatyczna**

ROZPORZĄDZENIE-Pojęcia

- „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
  tzw. PROCESOR
- Podmiot przetwarzający **przetwarza dane osobowe w imieniu administratora**. Procesor nie jest więc „właścicielem” danych otrzymanych od administratora w oznaczonym celu. Nie może ich wykorzystać do swoich celów. Wykonuje na powierzonych danych jedynie operacje zlecone przez administratora, jednocześnie zapewniając im dalszą ochronę, przewidzianą przepisami prawa.
- **Obowiązek zawarcia umowę o powierzenie przetwarzania danych osobowych**

ROZPORZĄDZENIE-Pojęcia

- „odbiorca” 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 (np. ZUS czy NFZ), które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

OBOWIĄZKI ADMINISTRATORA

ART. 30 rozporządzenia:

Prowadzenie rejestru czynności przetwarzania danych osobowych, za który odpowiada dany administrator

OBOWIĄZKI ADMINISTRATORA/uprawnienienia osób

OBOWIĄZEK INFORMACYJNY

- **Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:**
- **a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;**
- **b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;**
- **c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;**
- **d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;**
- **e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;**

OBOWIĄZKI ADMINISTRATORA/uprawnienienia osób

OBOWIĄZEK INFORMACYJNY

- **Poza informacjami, o których powyżej podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:**
- **a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;**
- **b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;**

OBOWIĄZKI ADMINISTRATORA/uprawnienienia osób

OBOWIĄZEK INFORMACYJNY

- **c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;**
- **d) informacje o prawie wniesienia skargi do organu nadzorczego;**
- **e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;**
- **f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.**

OBOWIĄZKI ADMINISTRATORA/PROCESORA

- **Artykuł 32. Bezpieczeństwo przetwarzania.**

  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,

OBOWIĄZKI ADMINISTRATORA/PROCESORA

- (...) w tym między innymi w stosownym przypadku:
- **a)** pseudonimizację i szyfrowanie danych osobowych;
- **b)** zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- **c)** zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- **d)** regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

OBOWIĄZKI ADMINISTRATORA/PROCESORA

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.

Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.

OBOWIĄZKI ADMINISTRATORA/PROCESORA

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 UWAGA ART. 29 ROZPORZĄDZENIA!!!

UPOWAŻNIENIE I ZWIĄZANIE POLECENIEM

Artykuł 29. Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego. Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

UPOWAŻNIENIE I ZWIĄZANIE POLECENIEM

- Upoważnienie udzielone przez administratora/procesora – brak samodzielności w zakresie decydowania o przetwarzaniu
- Polecenie wyłącznie administratora- zobowiązanie do stosowania się do takiego polecenia (zależność pomiędzy administratorem a osobą działającą z upoważnienia procesora;
- Osoba działająca z upoważnienia to nie tylko pracownik, ale także wolontariusz, praktykant, stażysta; osoba wewnątrz struktury administratora/procesora
- Upoważnienie wyraźne, a nie domniemane

UPOWAŻNIENIE I POLECENIE

- ROZPORZĄDZENIE NIE OKREŚLA FORMY UPOWAŻNIENIA (ale musi być udokumentowane)
- Umowa, lub inny instrument prawny, którego obligatoryjnym elementem jest zobowiązanie podmiotu przetwarzającego do przetwarzania danych wyłącznie na polecenie administratora
- Procesor MA OBOWIĄZEK POINFORMOWANIA ADMINISTRATORA O TYM, ŻE JEGO POLECENIE NARUSZA PRZEPISY ROZPORZADZENIA

ZMIANY

ABI / IOD

Wyznaczanie IODA

- **Artykuł 37 Wyznaczenie inspektora ochrony danych**

główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na **dużą skalę** szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO

- 5.1.1. Przetwarzanie nie jest przetwarzaniem na dużą skalę, o którym mowa w art. 35 ust. 3 lit. b) RODO gdy:
  - dotyczy jednoosobowej działalności gospodarczej prowadzonej przez osobę wykonującą zawód medyczny, w tym:
- jednoosobowej działalności gospodarczej jako indywidualnej praktyki lekarskiej, indywidualnej praktyki lekarskiej wyłącznie w miejscu wezwania, indywidualnej specjalistycznej praktyki lekarskiej, indywidualnej specjalistycznej praktyki lekarskiej wyłącznie w miejscu wezwania;

- dotyczy PWDL udzielających ambulatoryjnych świadczeń zdrowotnych, w tym w ramach Ambulatoryjnej Opieki Specjalistycznej, które zrealizowały świadczenia dla nie więcej niż 600 unikalnych pacjentów, w ostatnich 3 miesiącach (średnia z 3 poprzednich miesięcy) lub
- dotyczy PWDL udzielających wyłącznie świadczeń POZ i nie posiadających więcej niż 2750 przypisanych pacjentów w ostatnich 3 miesiącach (średnia z 3 poprzednich miesięcy).

Dotyczy PWDL udzielających stacjonarnych i całodobowych świadczeń zdrowotnych

- szpitalnych, które udzielały świadczeń zdrowotnych dla nie więcej niż 100 unikalnych pacjentów;
- innych niż szpitalne, które udzielały świadczeń zdrowotnych dla nie więcej niż 150 unikalnych pacjentów;

-w ostatnich 3 miesiącach (średnia z 3 poprzednich miesięcy).

Inspektor ochrony danych osobowych

Artykuł 37. Rozporządzenia.

- **Kwalifikacje:**
- Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.
- **Miejsce w strukturze organizacyjnej podmiotu**
- Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług

Inspektor ochrony danych osobowych

- **Artykuł 37 RODO**

Obowiązek publikacji danych kontaktowych

Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy

NP. NA STRONIE INTERNETOWEJ PODMIOTU LECZNICZEGO, W REGULAMINIE ORGANIZACYJNYM, NA TABLICY OGŁOSZEŃ

UODO------Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Status inspektora ochrony danych.

- Artykuł 38. Rozporządzenia

1. **Administrator oraz podmiot przetwarzający:**

- zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
- wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
- zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

Status inspektora ochrony danych.

Artykuł 38. Rozporządzenia

- Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia *(stąd obowiązek publikowania danych inspektora)*
- Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
- Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Wyznaczenie inspektora ochrony danych

Art. 10. [Zawiadomienie Prezesa Urzędu o wyznaczeniu inspektora]

Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora.

Wyznaczenie inspektora ochrony danych

Art. 10. [Zawiadomienie Prezesa Urzędu o wyznaczeniu inspektora]

Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora.

Zadania inspektora ochrony danych.

Artykuł 39. Rozporządzenia

1. Inspektor ochrony danych ma następujące zadania:

- a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

Zadania inspektora ochrony danych:

- d) współpraca z organem nadzorczym;
- e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
- 2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania

DONOSZENIE NA SAMEGO SIEBIE

- obowiązek powszechny, nałożony na każdego administratora danych osobowych oraz każdy podmiot przetwarzający dane (procesora).
- obowiązek informowania, przez te podmioty, UODO o naruszeniu przepisów ochrony danych osobowych. Termin jaki wyznacza europejski Ustawodawca został ustalony na 72h. Jeżeli w przeciągu tego czasu administrator nie powiadomi organu nadzorczego o naruszeniu w dalszym ciągu jest zobligowany to zrobić, podając przyczynę opóźnienia.
- Termin biegnie od momentu w którym administrator lub procesor dowie się o zaistniałym naruszeniu.

DONOSZENIE NA SAMEGO SIEBIE

- NARUSZENIE
- Przykładowo działanie lub zaniechanie, którego skutkiem jest zniszczenie bądź usunięcie danych, modyfikacja (zmiana treści); ujawnienie danych lub uzyskanie dostępu do nich przez osobę nieuprawnioną.

NARUSZENIE

- 50 tysięcy rekordów z danymi osobowymi (m.in. imię, nazwisko, adres, PESEL) i prawdopodobnie medycznymi (grupa krwi, diagnostyka) - takie poufne informacje wyciekły z Samodzielnego Zakładu Opieki Zdrowotnej

PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

- Artykuł 15 Prawo dostępu do danych osobowych
- Artykuł 16 Prawo do sprostowania danych
- Artykuł 17 Prawo do usunięcia danych ("prawo do bycia zapomnianym")
- Artykuł 18 Prawo do ograniczenia przetwarzania
- Artykuł 20 Prawo do przenoszenia danych
- Artykuł 21 Prawo do sprzeciwu

Środki ochrony prawnej, odpowiedzialność i sankcje

- **Artykuł 77. Prawo do wniesienia skargi do organu nadzorczego.**
- 1. Bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda 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 dotyczące narusza niniejsze rozporządzenie.
- 2. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 78.

Środki ochrony prawnej, odpowiedzialność i sankcje

- **Artykuł 78. Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu.**
- 1. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej.
- 2. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli organ nadzorczy właściwy zgodnie z art. 55 i 56 nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub efektach rozpatrywania skargi wniesionej zgodnie z art. 77.

Środki ochrony prawnej, odpowiedzialność i sankcje

- **Artykuł 79. Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu.**
- 1. Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. 77, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia.
- 2. Postępowanie przeciwko administratorowi lub podmiotowi przetwarzającemu wszczyna się przed sądem państwa członkowskiego, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną. Ewentualnie postępowanie takie może zostać wszczęte przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu, chyba że administrator lub podmiot przetwarzający są organami publicznymi państwa członkowskiego wykonującymi swoje uprawnienia publiczne.

Środki ochrony prawnej, odpowiedzialność i sankcje

- **Artykuł 80. Reprezentowanie osób, których dane dotyczą.**

Osoba, której dane dotyczą, ma prawo umocować podmiot, organizację lub zrzeszenie – które nie mają charakteru zarobkowego, zostały należycie ustanowione zgodnie z prawem państwa członkowskiego, mają cele statutowe leżące w interesie publicznym i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych – do wniesienia w jej imieniu skargi oraz wykonywania w jej imieniu praw, o których mowa w art. 77, 78 i 79, oraz żądania w jej imieniu odszkodowania, o którym mowa w art. 82, jeżeli przewiduje to prawo państwa członkowskiego.

ODSZKODOWANIE I ODPOWIEDZIALNOŚĆ

- **Artykuł 82. Prawo do odszkodowania i odpowiedzialność.**
- 1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.
- 2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

ODSZKODOWANIE I ODPOWIEDZIALNOŚĆ

- Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

  DOMNIEMANIE WINY NARUSZAJĄCEGO

- Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

- Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2.
- Postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem właściwym na mocy prawa państwa członkowskiego

ODSZKODOWANIE I ODPOWIEDZIALNOŚĆ

- Samodzielna podstawa roszczeń odszkodowawczych;
- Swoisty reżim odpowiedzialności odszkodowawczej;
- PRZESŁANKI ODPOWIEDZIALNOŚCI:
- SZKODA
- ZDARZENIE W WYNIKU KTÓREGO DOSZŁO DO POWSTANIA SZKODY (NARUSZENIE PRZEPISÓW RORPORZĄDZENIA)
- ZAISTNIENIE ZWIĄZKU POMIĘDZY NARUSZENIEM A SZKODĄ
- WYSTĄPIENIE WINY

ODSZKODOWANIE I ODPOWIEDZIALNOŚĆ

CIĘŻAR DOWODU wystąpienia naruszenia spoczywa na podmiocie, ale trzeba pamiętać o zasadzie ROZLICZALNOŚCI:

Art. 5 ust. 2 Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

KARY ADMINISTRACYJNE

- **Artykuł 83. Ogólne warunki nakładania administracyjnych kar pieniężnych.**
- 1. Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne, były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

KARY ADMINISTRACYJNE

- do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa,
- Do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa

KARY ADMINISTRACYJNE

Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a)–h) oraz j). Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:

a) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz 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 przez nich na mocy art. 25 i 32;

e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;

KARY ADMINISTRACYJNE

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;

i) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków;

j) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz

k) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

Ustawa o ochronie danych osobowych

- **Art. 107. [Nielegalne przetwarzanie danych osobowych]**
  1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
- 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej,podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

RODO-------CO ROBIĆ?

Co polecają eksperci?

- audyt wewnętrzny, aby ustalić stan faktyczny, czy obecnie dane są chronione zgodnie z przepisami i co ewentualnie wymaga poprawy. Dopiero wówczas można przejść do analizy, które obszary wymagają zmian w związku z wejściem w życie unijnego rozporządzenia i przeszkolić personel w tym zakresie.
- szkolenie całego personelu placówki medycznej, w którym trzeba mówić nawet o najprostszych kwestiach, nie tylko tych związanych z RODO. W dalszym ciągu bowiem zdarzają się incydenty związane z niewłaściwą ochroną danych osobowych, które nie powinny mieć miejsca przykładowo brak upoważnień dla lekarzy stażystów i studentów na przetwarzanie danych osobowych, lekceważenie obowiązku niszczenia danych wrażliwych w niszczarce itd.

KONIEC

Dziękuję za uwagę