



DAWID & PARTNERZY
ADWOKACI I RADCOWIE PRAWNI

Ochrona danych podmiotu leczniczego w kontekście RODO

Agenda

1

RODO a medyczne dane osobowe

2

Prawa pacjentów

3

Zabezpieczenie medycznych danych osobowych

4

Studium konkretnych przypadków

Dane osobowe w ochronie zdrowia



wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia konkretnej osoby



informacje pochodzące z badań laboratoryjnych/lekarskich części ciała lub płynów ustrojowych



dane genetyczne



próbki biologiczne



informacje o chorobie, niepełnosprawności, historii medycznej

RODO – ogólna charakterystyka

1

RODO – Rozporządzenie Ogólne o Ochronie Danych Osobowych

2

Rozporządzenie unijne (Parlament Europejski i Rada UE)

3

wiąże w całości od **25 maja 2018 r.**



RODO – ogólna charakterystyka

4

największa reforma ochrony danych osobowych od 21 lat

5

konieczność wdrożenia przez polskie podmioty szeregu zmian o charakterze prawnym i informatycznym



Q&A

Q&A



Czy zatrudniam pracowników?



Czy współpracuję z innymi podmiotami bądź lekarzami?



Czy przechowuję dokumenty zawierające dane osobowe?



Czy archiwizuję lub niszcze takie dokumenty?

Jeżeli na poprzednie pytania padły twierdzące odpowiedzi, to znaczy, że są Państwo albo administratorami, albo przedstawicielami administratorów.

Administrator



osoba fizyczna



osoba prawna



organ publiczny

lub inny podmiot, który
samodzielnie lub wspólnie
z innym (współadministratorzy)
ustala cele i sposoby przetwarzania
danych osobowych

Administrator



podmioty lecznicze (np. SPZOZ)



indywidualne czy też grupowe praktyki lekarskie
(prowadzone np. w formie prywatnych gabinetów
lekarskich, spółek)

I tak, w przypadku grupowej praktyki lekarskiej prowadzonej w formie spółki
(m.in. jawnej, partnerskiej) **administratorem będzie spółka, a nie lekarz.**

Administrator

Kodeks Cywilny:

Administratorem danych jest **podmiot** wykonujący **działalność leczniczą**, który **przetwarza** dane w **celach zdrowotnych**. Co do zasady, gdyż kodeks wskazuje, że nie może być administratorem danych tych pacjentów podmiot wykonujący działalność leczniczą, jeżeli **nie jest prawnie zobowiązany do prowadzenia, przechowywania i udostępniania dokumentacji medycznej** i ich ochrony we własnym imieniu i na własny rachunek, a który działa na rzecz innego podmiotu wykonującego działalność leczniczą



Przykładowo, administratorem nie będzie osoba wykonująca zawód medyczny, prowadząca jednoosobową działalność gospodarczą, pozostająca w stosunku prawnym z innym PWDL, w zakresie w jakim wykonuje swoje zadania w ramach działalności leczniczej prowadzonej przez ten PWDL w miejscu pobytu pacjenta (np. praktyka lekarska wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym prowadzącym ten zakład – z tymi podmiotami nie trzeba będzie także zawierać umowy powierzenia przetwarzani danych).

Przetwarzanie danych osobowych

Wszelkie operacje na danych osobowych dokonywane w sposób zautomatyzowany lub niezautomatyzowany, tj.:

- | | | | |
|---|----------------|----|---|
| 1 | zbieranie | 6 | adaptowanie lub modyfikowanie |
| 2 | utrwalanie | 7 | pobieranie |
| 3 | organizowanie | 8 | wykorzystywanie i przeglądanie |
| 4 | porządkowanie | 9 | ujawnianie przez przesyłanie lub innego rodzaju udostępnianie |
| 5 | przechowywanie | 10 | łączenie, dopasowywanie, ograniczenie, usuwanie i niszczenie |

Dotychczasowa ustawa o ochronie danych osobowych a RODO

Definicja przetwarzania danych osobowych:

Zgodnie z RODO:

„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;

Zgodnie z polską Ustawą:

rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Przetwarzanie danych osobowych

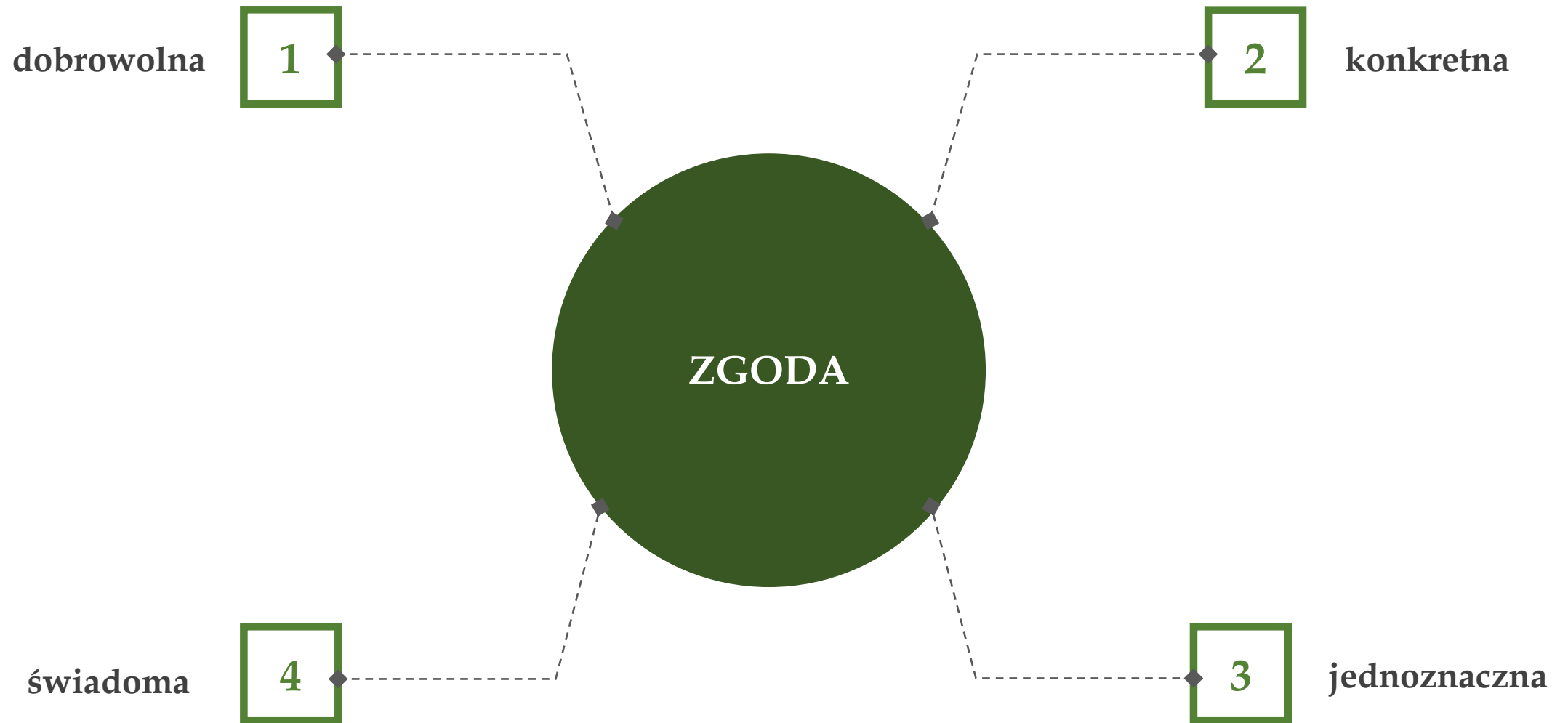
1

na podstawie normy prawnej (prawa UE lub państwa członkowskiego np. Kodeks pracy)

2

zgoda (oświadczenie lub wyraźne działanie) osoby, której dane dotyczą

Przetwarzanie danych osobowych



Przetwarzanie danych osobowych

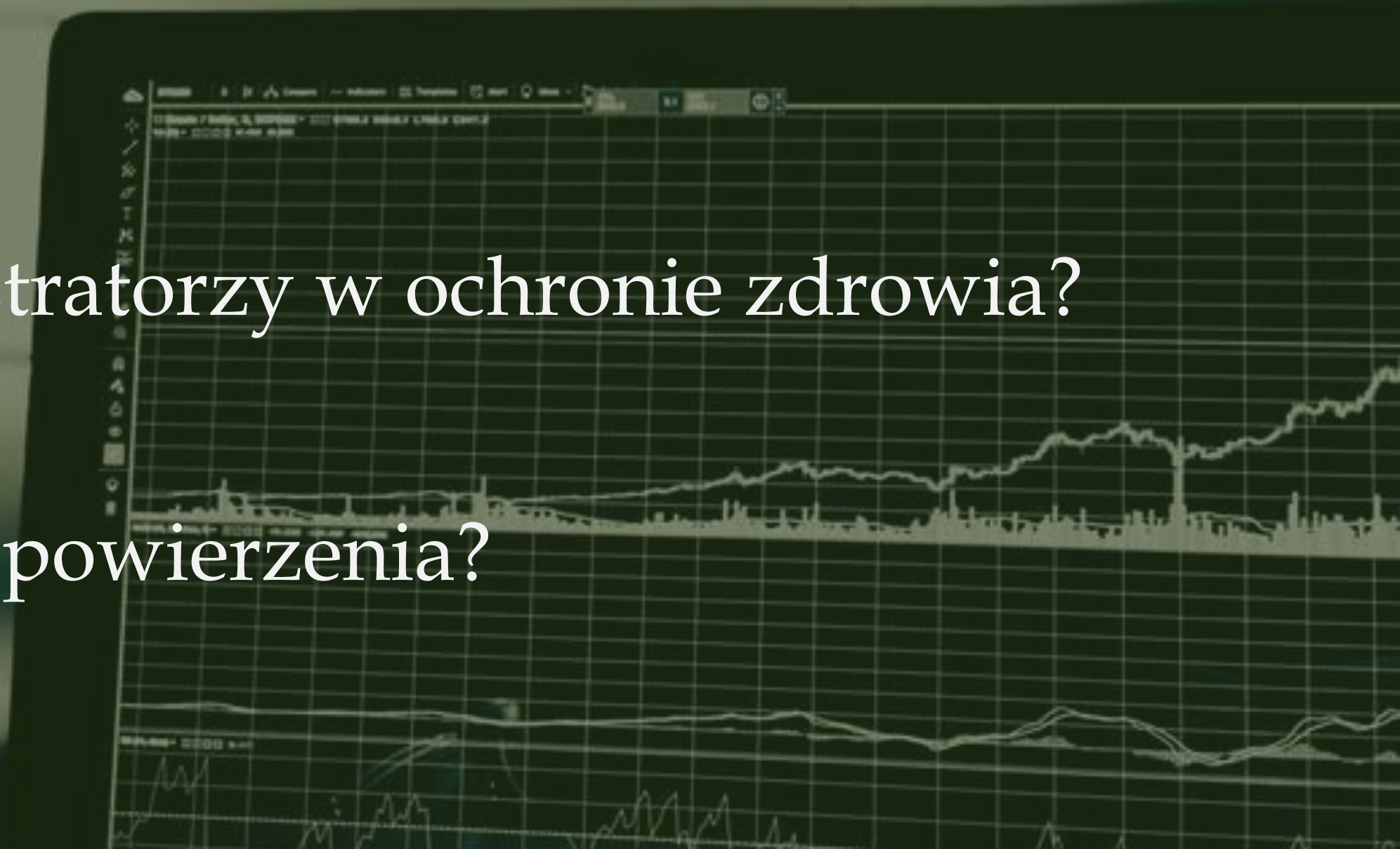
Zgodne z prawem również, gdy niezbędne do:

- wykonania umowy
- podjęcia działań na żądanie osoby, której dane dotyczą
- wypełnienia obowiązku prawnie ciążącego na administratora
- ochrony żywotnych interesów osoby, której dane dotyczą
- celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osobę trzecią

Podmioty przetwarzające / procesorzy

Administratorzy w ochronie zdrowia?

Umowy powierzenia?



Różnice pomiędzy administratorem a procesorem



Podmiot przetwarzający / procesor

- przetwarza w imieniu administratora
- obowiązek administratora wyboru odpowiedniego procesora (gwarancja ochrony danych osobowych)
- zgoda administratora – uprzednia, pisemna, jednoznaczna



Administrator a procesor

- kwestia decydowania o środkach i celach przetwarzania danych osobowych
- obowiązek zawarcia umowy powierzenia przetwarzania danych osobowych

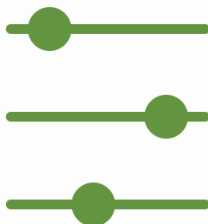
Umowa powierzenia przetwarzania



przedmiot i czas
trwania



kategorie
osób, które
dane dotyczą



rodzaj danych
osobowych

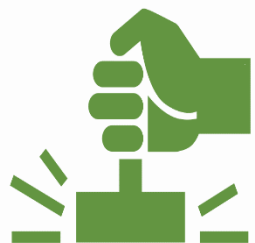


charakter i cel
przetwarzania



obowiązki i prawa
administratora

Dotychczasowa ustawa o ochronie danych osobowych a RODO



sankcje



zgłaszanie
wycieków danych
osobowych



ABI / IOD



zbiór danych osobowych

Nowa ustawa o ochronie danych osobowych

RODO zacznie obowiązywać niezależnie od wejścia w życie polskiej ustawy

Najważniejsze zmiany:

1

PUODO zamiast GODO

2

certyfikaty

3

uprawnienia kontrolera

4

zmiany w Kodeksie Pracy

Sankcje w RODO - maksymalne wysokości kar pieniężnych



OSOBY FIZYCZNE

- do 10 000 000 euro
- lub
- do 20 000 000 euro

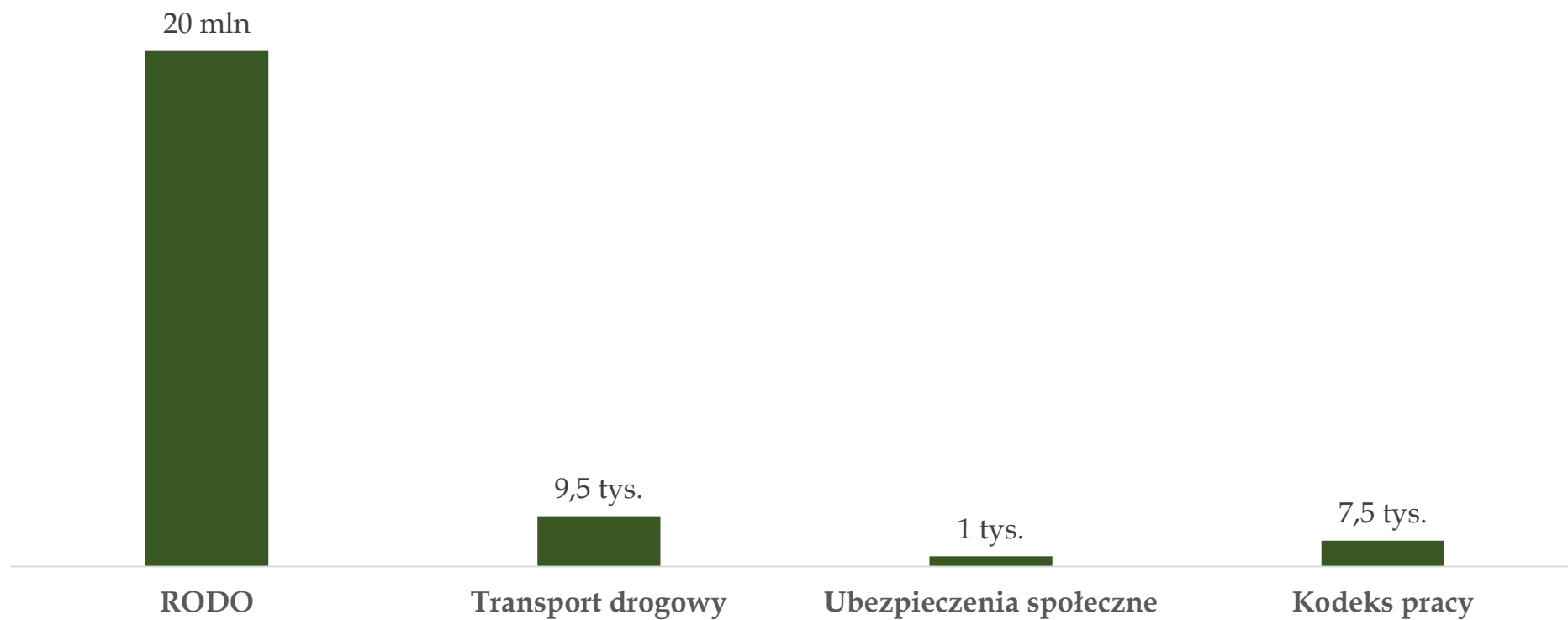


PRZEDSIĘBIORCY

- do 2% całkowitego rocznego globalnego obrotu z poprzedniego roku obrotowego lub do 10 000 000 euro
- lub
- do 4% całkowitego rocznego globalnego obrotu z poprzedniego roku obrotowego lub do 20 000 000 euro

Kary z RODO na tle innych kar

Maksymalne wysokości kar pieniężnych
za naruszenia przepisów ustawy*



*Powyższe kwoty podane są w EUR według kursu 1 EUR = 4,27 PLN

Inne sankcje w RODO

1

odszkodowanie za poniesioną
szkodę dla pokrzywdzonego

2

ostrzeżenia, upomnienia

3

zakaz lub ograniczenie przetwarzania
danych osobowych

3

nakazy

Agenda

1

RODO a medyczne dane osobowe

2

Prawa pacjentów

3

Zabezpieczenie medycznych danych osobowych

4

Studium konkretnych przypadków

Nowe prawa pacjentów w RODO



prawo do informacji (obowiązek informacyjny)



prawo dostępu do danych



prawo uzyskania kopii przetwarzanych danych



prawo do uzupełnienia bądź sprostowania danych



prawo do bycia zapomnianym



prawo do przenoszenia danych



sprzeciw wobec przetwarzania

Obowiązki informacyjne Administratora

Obowiązki administratora

1. dane administratora i dane kontaktowe (przedstawiciela, IOD)
2. cel i podstawa prawna przetwarzania
3. odbiorcy danych
4. zamiar przekazania do państwa trzeciego lub organizacji międzynarodowej
5. okres, przez jaki będą przechowywane
6. pouczenie o prawie modyfikacji, uaktualnienia, ograniczenia przetwarzania, usunięcia bycia zapomnianym, wniesienia skargi do PUODO
7. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu

Obowiązek informacyjny – c.d.

poinformować o przysługujących prawach (np. żądania dostępu do danych osobowych, sprostowania i uzupełnienia danych osobowych, bycia zapomnianym, żądania ograniczenia przetwarzania, przenoszenia danych, sprzeciwu wobec przetwarzania).



Powyższe informacje powinny zostać przekazane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Obowiązek informacyjny może zostać spełniony poprzez indywidualne udostępnienie każdemu pacjentowi stosownego oświadczenia (w formie papierowej bądź elektronicznej) lub zamieszczenie go w ogólnodostępnym miejscu jak np. w rejestracji, poczekalni, na izbie przyjęć, na stronie internetowej.

Tajemnica lekarska



Co do zasady, **inne podmioty** mają również **obowiązek przekazania niektórych informacji osobom w przypadku zbierania danych osobowych niebezpośrednio od nich**. Taka sytuacja zachodzi m.in. w związku z udostępnieniem dokumentacji medycznej zawierającej dane np. osób **najbliższych, przedstawicieli ustawowych czy osób upoważnionych do wglądu w dokumentację pacjenta**. Powyższy przypadek nie dotyczy jednak podmiotów wykonujących działalność leczniczą, które nie są zobligowane do udostępniania takich informacji ze względu choćby na tajemnicę lekarską, co znalazło wyraz w art. 14 ust. 5. lit. c) i d) RODO.



Prawo dostępu do danych



prawo do informacji o stanie zdrowia i prawo dostępu do dokumentacji medycznej



maksymalnie 2 miesiące



możliwość odmowy podjęcia jakichkolwiek działań ze względu na ewidentnie nieuzasadnione lub nadmierne żądanie osoby



bezpłatna kopia przetwarzanych danych



opłata za kolejne nie wyższa niż opłaty określone w art. 28 ust. 5 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.



drogą tradycyjną „papierową” lub elektroniczną

Sprostowanie i uzupełnienie danych

1

uprawnienie do niezwłocznego sprostowania lub uzupełnienia przekazanych danych osobowych

2

nie może dotyczyć wpisów, których zmiana naruszyłaby autonomiczność zawodową osoby wykonującej zawód medyczny

Prawo do bycia zapomnianym

1

nie znajdzie zastosowania wobec danych osobowych pacjentów przetwarzanych na podstawie art. 9 ust. 2. lit. h) (niezbędne do celów m.in. profilaktyki zdrowotnej lub medycyny pracy, zapewnienia opieki zdrowotnej, leczenia)

2

administrator ma obowiązek przechowywania danych w ramach dokumentacji medycznej przez 20 lat z pewnymi wyjątkami.

3

jeżeli pacjent żąda usunięcia danych, na których przetwarzanie wyraził zgodę, prawo to powinno zostać zrealizowane, ale wyłącznie w zakresie danych podanych fakultatywnie.

Prawo do przenoszenia danych

Pomimo braku obowiązku administratora zrealizowania prawa do przenoszenia danych w ramach przetwarzania określonego w art. 9 ust. 2. lit. h), tj. niezbędnego do m.in.

- zapewnienia opieki zdrowotnej
- leczenia
- zarządzania systemami i usługami opieki zdrowotnej

powinien on poinformować pacjenta o zasadności i podstawie prawnej odmowy oraz o możliwości uzyskania dostępu do dokumentacji.



NALEŻY PAMIĘTAĆ, ŻE ŻĄDANIE PRZENOSZENIA DANYCH JEST ZASADNE TYLKO POD PEWNYMI WARUNKAMI:

- gdy przetwarzanie nie obejmuje działalności opisanej w art. 9 ust. 2. lit. h
- gdy odbywa się w sposób zautomatyzowany (wyłącznie w systemach informatycznych, a nie w formie papierowej)
- na podstawie zgody pacjenta lub umowy zawartej z podmiotem wykonującym działalność leczniczą.

Sprzeciw wobec przetwarzania

- Pacjent może zgłosić się także ze sprzeciwem do administratora wobec przetwarzania danych osobowych.
- Żądanie będzie trafne, jeśli pacjent zastosuje je wobec danych przetwarzanych w celu wykonywania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej bądź w celu wynikającym z prawnie uzasadnionych interesów administratora.

Sprzeciw wobec przetwarzania



Pacjent może zgłosić się także ze sprzeciwem do administratora wobec przetwarzania danych osobowych. Żądanie będzie trafne, jeśli pacjent zastosuje je wobec danych przetwarzanych w celu wykonywania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej bądź w celu wynikającym z prawnie uzasadnionych interesów administratora.

Przedstawione obowiązki administratora skorelowane z uprawnieniami pacjentów **powinny znaleźć swoje odzwierciedlenie w dokumentach opisujących ochronę danych osobowych w danym podmiocie**. W ich treści należy również **zawrzeć charakterystykę wewnętrznych procedur** wprowadzonych w celu zrealizowania i zagwarantowania podstawowych praw wynikających z unijnego rozporządzenia.

Agenda

1

RODO a medyczne dane osobowe

2

Prawa pacjentów

3

Zabezpieczenie medycznych danych osobowych

4

Studium konkretnych przypadków

Ocena skutków dla ochrony danych



systematyczny opis
planowanych operacji
przetwarzania i celów
przetwarzania



ocena ryzyka naruszenia praw lub
wolności osób, których dane dotyczą



ocena, czy operacje
przetwarzania są niezbędne



środki planowane w celu zaradzenia
ryzyku, w tym zabezpieczenia oraz
środki i mechanizmy bezpieczeństwa



ocena, czy operacje
przetwarzania są
proporcjonalne w stosunku do
celów

Bezpieczeństwo fizyczne



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 niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądowi i uaktualniane.



identyfikatory osobowe



system monitoringu wizyjnego



czujniki temperatury i wilgoci



system alarmowy przeciwwłamaniowy

Bezpieczeństwo systemów informatycznych



identyfikator użytkownika



hasła



cykliczny przegląd uprawnień



zapisywanie danych na udziałach sieciowych



**min. 8 znaków, małe i wielkie litery,
cyfry, znaki specjalne**

Agenda

1

RODO a medyczne dane osobowe

2

Prawa pacjentów

3

Zabezpieczenie danych osobowych medycznych

4

Studium konkretnych przypadków

Czy zgodne z RODO?



Opaski dla noworodków?



Karty informacyjne pacjenta przy łóżku?



Udzielanie informacji przez telefon?



Wydawanie wyników badań innym osobom niż pacjentowi?

Czy wymagane?



Anonimowe kroplówki?



Specjalne strefy oddzielające oczekujących do rejestracji?



Usunięcie danych na życzenie pacjenta?



Nieumieszczanie przed gabinetem listy z nazwiskami zapisanych pacjentów?

DZIĘKUJEMY ZA UWAGĘ.