# RODO

**(Rozporządzenie o Ochronie Danych Osobowych)**

## Przetwarzanie danych szczególnych w medycynie – nowe regulacje

# Ochrona Danych Osobowych

Ma być bezpiecznie!

Akty prawne:

Krajowe:
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r.

Europejskie:
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 (ogólne rozporządzenie o ochronie danych)

# RODO - Rozporządzenie o Ochronie Danych Osobowych

## 10 najważniejszych zmian, które wprowadza RODO

- Bezpośrednia odpowiedzialność przetwarzającego dane
- Zgłaszanie naruszeń
- Nowe rozszerzone prawa obywateli
- Ograniczenie profilowania
- Wyznaczenie Inspektora Ochrony danych Osobowych
- Inwentaryzacja danych i wymagania wobec dokumentacji
- Zgody
- Rozbudowanie obowiązku informacyjnego
- Ocena wpływu ochrony danych
- Transfer danych poza Unię Europejską

# Podstawowe pojęcia art. 4

**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;

**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;

**Zbiór danych**

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

Dane osobowe:
- zwykłe
- szczególne (wrażliwe)

Dokumentacja z danymi:
- tradycyjna (papierowa)
- elektroniczna

# Zasady przetwarzania danych osobowych

| | |
|---|---|
| Zgodność | przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem i gdy osoba wyraziła zgodę”); |
| Ograniczenie celu | 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 |
| Minimalizacja danych | adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane |
| Prawidłowość | 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 |
| Ograniczenie celu | 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 |
| Integralność i poufność | 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 |
| Rozliczalność | Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie |

# Rejestr czynności przetwarzania danych

**Rejestr czynności** zastąpił **obowiązek zgłaszania** zbiorów danych do organu nadzorczego (obecnie UODO).
Rejestr będzie sporządzany wewnątrz przedsiębiorstwa albo innej instytucji prywatnej bądź publicznej, a dokumentacja z rejestru pozwoli rozliczać się przed organem nadzoru w przypadku kontroli.
W rejestrze tym zamieszcza się wszystkie następujące informacje:

- **Imię i nazwisko lub nazwę oraz dane kontaktowe administratora**
- **Cel przetwarzania**
- **Opis kategorii osób**
- **Kategorie odbiorców**
- **Planowane terminy usunięcia poszczególnych kategorii danych**
- **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**

<u>Wyjątki</u>
Rejestr czynności, nie musi być prowadzony w przedsiębiorstwach zatrudniających **mniej niż 250 osób**, chyba że:
- przetwarzanie może naruszać **prawa lub wolności osób**, których dane przetwarzamy np. może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości,
- przetwarzanie obejmuje **szczególne kategorie danych (np. dane biometryczne) lub dane dotyczące wyroków skazujących i naruszeń prawa**,
- przetwarzanie nie ma charakteru sporadycznego, np. przetwarzanie danych związanych z zarządzaniem Klientami, zarządzaniem Personelem.

**Rejestr w postaci pliku w dowolnym formacie**

# Obowiązek zgody na przetwarzanie danych

## Zgoda zgodna zasadami w RODO

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.

## Uzyskanie zgody dziecka

**Zgoda wymagana do 16 roku życia dziecka**

Jeżeli dziecko nie **ukończyło 16 lat**, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

## Czy stara zgody obowiązują - TAK

Zgodnie z RODO, jeżeli przetwarzanie ma za podstawę zgodę w myśl dyrektywy 95/46 i odpowiada ona warunkom przewidzianym w ustawie o ochronie danych osobowych z 1997 r. będzie ona ważna również po 25 maja 2018 r. W takim przypadku administrator może kontynuować przetwarzanie w oparciu o „starą” zgodę.

# PSEUDONIMIZACJA

**Pseudonimizacja** - to „ukrycie” danych osobowych, ponieważ nadal istnieje narzędzie, które pozwala je odczytać. Dane osobowe, które są spseudonimizowane, pozostają danymi osobowymi. Poddając je pseudonimizacji, tylko na jakiś czas „ukrywamy” informacje pozwalające zidentyfikować osobę, której dane dotyczą. **Aby dokonać skutecznie czynności pseudonimizacji istotne jest to, aby klucz pozwalający odczytać dane był przechowywany osobno, tj. w innym miejscu, niż same dane. Ponadto, klucz musi być odpowiednio zabezpieczony w sposób techniczny i organizacyjny.**

Pacjent 12 178

- Identyfikator

Imię - Jan
Nazwisko – Kowalski
Data urodzenia: 20.03.1988
PESEL: 88032012345
Tel. 792838383
Data 1 wizyty: 03.03.2016
Identyfikator: Pacjent 12 178

- Informacja w programie kadrowo-płacowym oraz wykazie osób upoważnionych do przetwarzania danych osobowych

# Bezpieczne przetwarzanie dokumentacji medycznej - zagrożenia

- Nieuprawniony dostęp przez użytkowników
- Nieuprawniony dostęp przez osoby z zewnątrz
- Nieuprawnione wykorzystanie aplikacji przetwarzającej informacje na temat pacjentów
- Możliwość uszkodzenia lub wprowadzenia do systemu destrukcyjnego oprogramowania obejmującego np. wirusy, lub innego złośliwego oprogramowania
- Brak świadomości zagrożeń
- Błąd ludzki – główne zagrożenie danych

# Zgłaszanie naruszeń zgodnie z przepisami RODO

**Dokumentowanie naruszeń ochrony danych osobowych**

**Bezwzględne zgłoszenie incydentu w ciągu 72 godzin**

## Zgłoszenie

- opis naruszenia
- opis konsekwencji
- opis środków zaradczych

W przypadku, kiedy naruszenie może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator musi bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą.

**wyjątki**

Przypadki kiedy nie musimy zgłaszać naruszeń osobom, których dane przetwarzamy są następujące:

- administrator zastosował odpowiednie środki techniczne i organizacyjne dla danych których dotyczy naruszenie, takie jak szyfrowanie, aby uniemożliwić osobom nieuprawnionym odczytanie danych,
- administrator w dalszej kolejności użył środków, które eliminują prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
- administrator musiałby dokonać niewspółmiernie dużego wysiłku by powiadomić osobę której dane dotyczą o naruszeniu, wówczas wydawany jest publiczny komunikat lub inny podobny środek by poinformować osoby w skuteczny sposób.

# Bezpieczne przetwarzanie dokumentacji medycznej – zabezpieczenia techniczne systemów i sprzętu

Bezpieczeństwo systemów teleinformatycznych:

- Ocenianie skuteczności środków technicznych
- Ocenianie środków organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych medycznych
- Stosowanie oprogramowania ograniczającego dostęp do sieci wewnętrznej z zewnątrz – np. Firewall
- Stosowanie oprogramowania antywirusowego – np. ESET lub inny antywirus
- Stosowanie oprogramowania monitorującego ruch w sieci wewnętrznej czyli kto i jakie dane kopiuje drukuje np. Statlook ma moduł RODO

# Bezpieczne przetwarzanie dokumentacji medycznej – zabezpieczenia danych medycznych

Różne zabezpieczenia danych medycznych:

- Dostęp do komputera: użytkownik i hasło nadane przez Administratora
- Autoryzowany dostęp do aplikacji medycznej: identyfikator i hasło nadane przez Administratora
- Szyfrowanie nośników informacji z danymi np. pendrive czy dysk zewnętrzny
- Stosowanie hasła na plikach z danymi osobowymi
- Archiwizacja danych zgodnie z przepisami prawa
- Czy jest zachowana poufność transamisji (dane w transporcie czy są szyfrowane)

Bezpieczne przetwarzanie dokumentacji medycznej – archiwizacja danych medycznych
Backup polisą ubezpieczeniową XXI w.

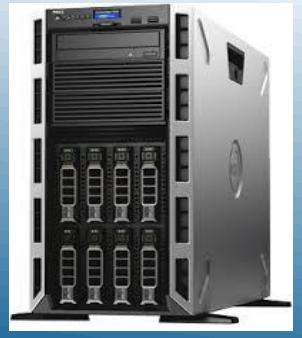
Różne archiwizacji danych medycznych:

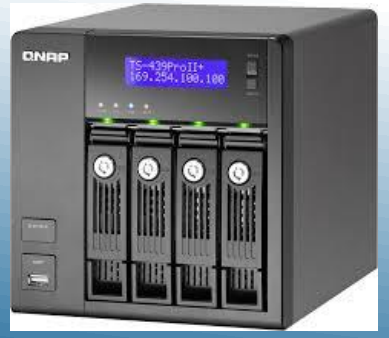
- Archiwizacja i przechowywanie zgodne z przepisami prawa

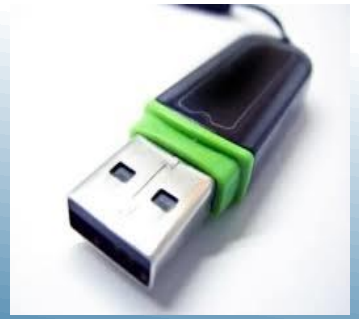
- Robienie pełnej kopii zapasowej (Full Backup)

- Zaplanowanie przechowywania kopii zapasowych na serwerach backupowych lub zewnętrznych nośnikach danych zaszyfrowanych i odpowiednio zabezpieczonych przed dostępem osób nieuprawnionych

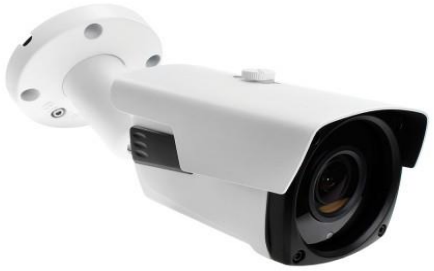
Dokładne zaplanowanie i przygotowanie strategii kopii zapasowych jest pierwszym krokiem w celu stworzenia prawidłowo funkcjonującego procesu backupu. We współczesnym świecie okazuje się on szczególnie istotny w funkcjonowaniu osób, które przechowują wiele cennych informacji.

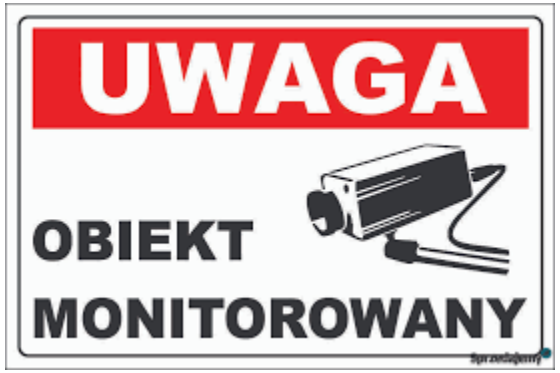


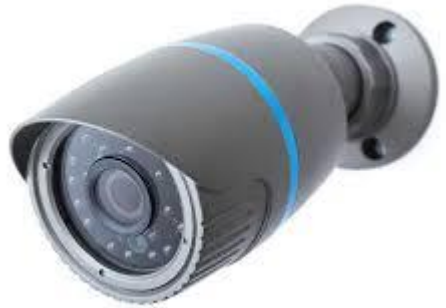


# Monitoring wizyjny





- Monitoring wizyjny może być wykorzystywany w określonych celach. Jeżeli monitorujesz po to, żeby zapewnić bezpieczeństwo osób, żeby zapewnić bezpieczeństwo mienia, żeby chronić tajemnice prawnie chronione, wtedy monitoring w większości przypadków będzie dozwolony.

- A co powinni zrobić pracodawcy chcący korzystać z monitoringu? Przede wszystkim powinni stworzyć i stosować odpowiednią procedurę przewidzianą w regulaminie pracy.

- Monitoringu być nie powinno. Są to m.in. toalety, szatnie czy przebieralnie. - To miejsca, które ze względu na ochronę naszej intymności rzeczywiście powinny być traktowane szczególnie.

# Wdrażamy RODO co musimy wiedzieć

Ważne

- Jak bezpiecznie przechowywać dokumentację medyczną?
- Kto oprócz osób wykonujących zawód medycznych, jest uprawniony do przetwarzania danych zawartych w dokumentacji medycznej?
- Jak budować bezpieczeństwo elektronicznej dokumentacji medycznej?
- Jakie grożą kary za przetwarzanie medycznych danych osobowych których przetwarzanie jest niedopuszczalne, albo dokonywane przez nieuprawnione do tego osoby?
- Jakie czynności mogą być nieuprawnionym ujawnieniem informacji zawartych w dokumentacji medycznej?
- Jakie sankcje wprowadza ogólne rozporządzenie unijne za nieuprawnione udostępnienie danych osobowych (nawet jeśli było nieumyślne)?
- Jakie zapisy musi mieć umowa o powierzeniu przetwarzania danych osobowych medycznych wynikające z ustawy o ochronie danych osobowych a także przepisów sektorowych?
- Jakie elementy powinien mieć system fizycznego zabezpieczenia danych osobowych w jednostkach medycznych?
- Jak skutecznie oddzielać dane medyczne od osobowych danych medycznych, tam gdzie jest to możliwe (np. na Karcie Medycznych Czynności Ratunkowych)?

# RODO - Rozporządzenie o Ochronie Danych Osobowych - wdrożenie

Ma być bezpiecznie!

Wszystko zaczyna się od ludzi

Administrator danych i pracownicy w firmie

Plan Audytu + Harmonogramy czynności + Komunikacja o planowanych działaniach

Analiza wyników audytu + Ocena + Co musimy zrobić

Plan wdrożenia + Ocena charakteru firmy + Ocena ryzyka + Możliwości finansowe

Proces wdrażania w firmie

… i kończy na ludziach

# Edukacja – najskuteczniejsza broń do ochrony naszych danych

Nasza wiedza o potrzebie ochrony danych osobowych nie jest, niestety, imponująca. Wiemy, ile problemów może spowodować utrata dowodu osobistego lub innego dokumentu tożsamości, ale już skutki kradzieży naszych danych w wersji elektronicznej kojarzą nam się co najwyżej z atakiem hakerów na internetowe konto bankowe. Dlaczego tak się dzieje? Czego nie wiemy, a powinniśmy, o ochronie naszych danych? Czy przestępcy wiedzą o niej więcej niż my sami?

Dziękuję za uwagę