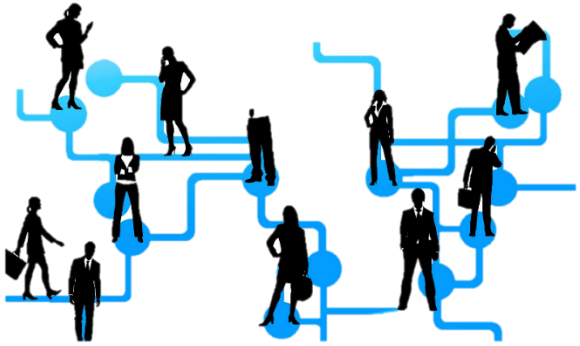
Centrum Danych Osobowych

RODO
WYMOGI OCHRONY DANYCH OSOBOWYCH PACJENTÓW MLD

Katowice, dnia 24 kwietnia 2018 r.



r. pr. Michał Rytel

PODSTAWA PRAWNA

§ **Konstytucja Rzeczpospolitej Polskiej** z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483)

§ **Ustawa** z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.)

§ **Rozporządzenie** Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji

§ **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji** z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

CZYM JEST DANA OSOBOWA?

Dane osobowe to szczególny typ informacji związanych z **osobami fizycznymi**. Daną osobową jest wszelka informacja dotycząca zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

- imię i nazwisko
- adres zamieszkania
- numer PESEL lub NIP
- dane osób fizycznych prowadzących działalność gospodarczą, dostępne powszechnie w CEIDG

- dane dotyczące podmiotów, spółek, fundacji, stowarzyszeń i innych informacji odnoszących się do podmiotów innych niż osoby fizyczne

DANE WRAŻLIWE

szczególna kategoria danych osobowych – bardziej rygorystyczna ochrona niż ochrona „zwykłych" danych osobowych

ich przetwarzanie jest codziennością

należy zwracać **szczególną uwagę i daleko idącą ostrożność** w ich przetwarzaniu - dane te głęboko ingerują w życie prywatne, a ich ujawnienie może nieść za sobą poważne, negatywne konsekwencje

DANE WRAŻLIWE

Dane wrażliwe jako szczególna kategoria danych

- pochodzenie rasowe lub etniczne
- poglądy polityczne
- przynależność wyznaniowa, partyjna lub związkowa
- przekonania religijne lub filozoficzne
- kod genetyczny
- STAN ZDROWIA !!!
- nałogi
- życie seksualne
- skazania
- orzeczenia o ukaraniu
- mandaty, orzeczenia wydane przed sądem lub urzędem

Dlaczego chronimy dane osobowe?

obowiązek ustawowy – za naruszenie grożą poważne konsekwencje prawne

dbamy o interes tych, których dane dotyczą i zwiększamy ich zaufanie

dbamy o interes nasz i naszego pracodawcy - chronimy dobre imię

PRZETWARZANIE

Przetwarzanie danych osobowych to wszelkie operacje na danych osobowych

zbieranie (gromadzenie)

przechowywanie

udostępnianie

zmienianie

przekazywanie

utrwalanie

usuwanie (niszczenie, modyfikacja)

opracowywanie

OCHRONA

Forma, w której przetwarzane są dane

Bez względu na formę przetwarzania, dane należy chronić z jednakową starannością!

W formie tradycyjnej (papierowej):
w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych

W formie elektronicznej:
w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych

RODO

Rozporządzenie Parlamentu Europejskiego i Rady (UE)

§ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/697 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zwane „ogólnym rozporządzeniem o ochronie danych" lub „RODO"

§ Rozporządzenie unijne zostało uchwalone 27 kwietnia 2016 r., weszło w życie 17 maja 2016 r., natomiast 25 maja 2018 r. zacznie obowiązywać bezpośrednio w porządkach krajowych.

RODO

PODSTAWOWE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Centrum Danych Osobowych

- zasada legalności (zgodności z prawem), rzetelności i przejrzystości,
- zasada ograniczenia celu,
- zasada minimalizacji danych,
- zasada prawidłowości (poprawności),
- zasada ograniczenia przechowywania,
- zasada zapewnienia bezpieczeństwa danych.

RODO

CO NALEŻY PRZYGOTOWAĆ?

Szkolenia	Rejestr czynności przetwarzania	Privacy by design (tworzenie dokumentacji)	Privacy by default (maksymalna ochrona danych)
Procedura notyfikacji naruszeń	Inspektor Ochrony Danych	Analiza ryzyka	Wewnętrzne procedury i polityki
Klauzule zgody	Pseudonimizacja	Obowiązek informacyjny	Ewidencja zgód
Ocena skutków planowania operacji przetwarzania dla ochrony danych	Analiza umów powierzenia	Konsultacje z organem nadzoru	Nowe prawa podmiotów danych

RODO

OBOWIĄZKI PRZED 25 MAJA 2018 ROKU

- Audyt - w celu określenia stanu i efektywności systemu zabezpieczeń oraz identyfikacji potencjalnych zagrożeń.
- Przygotowanie polityk i procedur funkcjonujących wewnątrz organizacji – w celu dostosowania się do wymagań RODO
- Przygotowanie rejestrów czynności przetwarzania danych– w celu możliwości sprawowania efektywnej kontroli i wdrożenia właściwych środków ochrony
- Przygotowanie wzorów oświadczeń i klauzul zgody – w celu zabezpieczenia procesu przetwarzania danych
- Powołanie IOD lub zamiana ABI w IOD
- Stworzenie mechanizmu wykrywania i notyfikacji naruszeń – w celu realizacji nowych wymagań RODO i przygotowania środków ochrony przed potencjalnymi roszczeniami lub sankcjami
- Przeprowadzenie szkoleń z zakresu ochrony danych osobowych

RODO

NOWOŚCI ☺

Nowość! Obowiązek zgłaszania naruszeń bezpieczeństwa przetwarzania danych do organu nadzorczego!
72 h po stwierdzeniu naruszenia – czas na zgłoszenie naruszenia do organu nadzorczego, chyba że jest mało prawdopodobne by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Ważne! Ciężar wykazanie, że naruszenie nie powoduje naruszenia praw lub wolności spoczywa na naruszającym!

Nowość! Obowiązek zawiadomienia osoby, której dane uległy naruszeniu!
Gdy naruszenie ochrony danych może powodować wysokie ryzyko naruszenia praw lub wolności osoby fizycznej, administrator danych zobowiązany jest powiadomić, oprócz organu nadzorczego, także osobę, której dane dotyczą.

RODO

KARY ☹

Ważne!

Naruszenie zasad ochrony danych osobowych lub niezgłoszenie naruszenia organowi nadzorczemu w wyznaczonym czasie będzie skutkować nałożeniem kary grzywny w kwocie **do 10 000 000 euro** lub do 2% całkowitego rocznego światowego obrotu przedsiębiorstwa – przy czym zastosowanie będzie miała kara wyższa.

RODO nie określa formy zgłoszenia, ta kwestia została pozostawiona do uregulowania przez państwa członkowskie

RODO

NOWA NAZWA DLA GIODO

Dotychczasowy GIODO – Generalny Inspektor Ochrony Danych Osobowych – zyska nową nazwę: Prezes Urzędu Ochrony Danych Osobowych (UODO)

Prezes Urzędu będzie udzielać zaleceń dotyczących szczególnych operacji przetwarzania (art. 57 ust. 1 Rozporządzenia).

Nowe przepisy dotyczące organów stanowią o:

- przyjmowaniu standardowych klauzul umownych,
- prowadzeniu wykazu ocen skutków przetwarzania,
- udzielaniu zaleceń jak przetwarzać dane osobowe, o których mowa w art. 36 ust. Rozporządzenia w związku z uprzednimi konsultacjami,
- zachęcaniu do tworzenia i stosowania kodeksów postępowania,
- zachęcaniu do mechanizmów certyfikacji (dziś nie istnieją),
- akredytacji podmiotów certyfikujących,
- prowadzeniu rejestru naruszeń,
- obowiązku wzajemnej pomocy i współpracy z innymi organami nadzorczymi.

RODO

INSPEKTOR OCHRONY DANYCH OSOBOWYCH (IOD)

- Obecnie powołanie ABI jest fakultatywne, RODO natomiast określa sytuacje kiedy powołanie IOD będzie obligatoryjne.

  Kryterium wyznaczania IOD: kwalifikacje zawodowe, a w szczególności wiedza na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia powierzonych mu zadań.

- Znacznie szerszy zakres obowiązków IOD w stosunku do ABI.
  Funkcję IOD można powierzyć pracownikowi albo zewnętrznemu podmiotowi na podstawie umowy o świadczenie usług.

- IOD może wykonywać inne zadania i obowiązki w organizacji tylko jeżeli wykonywanie takich zadań i obowiązków nie powoduje konfliktu interesów.

RODO

Inspektor zobowiązany będzie m.in. do:

- informowanie administratora oraz pracowników o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów,
- monitorowanie przestrzegania Rozporządzenia oraz innych przepisów Unii i państw członkowskich oraz polityk administratora lub procesora,
- szkolenie personelu uczestniczącego w operacjach przetwarzania
- przeprowadzania systematycznych audytów w organizacji, w której został powołany,
- udzielania wskazówek administratorowi w przedmiocie wdrożenia odpowiednich i skutecznych środków technicznych jak również organizacyjnych mających zabezpieczyć dane osobowe oraz jak wykazać przestrzeganie prawa przez administratora lub podmiotu przetwarzającego dane w szczególności jeżeli chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę pod katem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko,
- udzielania na żądanie zaleceń co do oceny skutków oraz monitorowanie ich wykonania w przypadku, gdy administrator danych przed rozpoczęciem przetwarzania zobowiązany jest do przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych.

Nowością przewidzianą w rozporządzeniu jest możliwość wyznaczenia jednego inspektora danych przez grupę grupa przedsiębiorców oraz przez organy lub podmioty publiczne.

RODO

UWAGA WYSOKIE SANKCJE

Za naruszenie istotnych przepisów ochrony danych osobowych, Rozporządzenie przewiduje grzywnę **do 20 mln EUR,** a w przypadku przedsiębiorstwa – do 4% całkowitego światowego obrotu z poprzedniego roku. Niższe kary do 10 mln EUR lub do 2% światowego obrotu, przewidziane są w sprawach mniejszej wagi.

Każdy przypadek będzie indywidualnie rozpatrywany i pod uwagę będą brane m.in. następujące elementy:

- skala naruszenia,
- umyślność działań,
- co zrobiono, żeby zminimalizować szkody poniesione przez osoby, których dane dotyczą,
- „recydywa", czyli czy jest to pierwsze, czy kolejne przewinienie,
- kategorie przetwarzanych danych osobowych,
- stopień współpracy z GIODO.

RODO

NOWE PRZEPISY OBEJMUJĄCE PROCESORA

Procesor = podmiotu przetwarzającego dane w imieniu administratora danych

- Nie będzie wolno powierzać dalej przetwarzania danych osobowych bez zgody administratora
- Podmiot przetwarzający (procesor) w razie stwierdzenia, iż doszło do naruszenia ochrony danych osobowych, zgłasza je administratorowi i nie musi ich zgłaszać do UODO.
- Obowiązkiem podmiotu przetwarzającego będzie prowadzenie rejestru wszelkich kategorii czynności przetwarzania, dokonywanych w imieniu administratora
- Procesor będzie miał również obowiązek udostępnić taki rejestr na żądanie UODO, a także powołać inspektora ochrony danych osobowych, jeśli zaistnieje przynajmniej jeden z czynników, o których stanowi art. 37 ust. 1 Rozporządzenia.

Pseudonimizacja danych

RODO definiuje proces pseudonimizacji jako przetwarzanie danych osobowych w taki sposób, aby nie było możliwe zidentyfikowanie, do kogo one należą, bez dostępu do innych informacji, przechowywanych bezpiecznie w innym miejscu. Polega on na zastępowaniu jednego atrybutu (bardzo często nietypowego) w zapisie innym atrybutem. W założeniu proces pseudonimizacji powinien być odwracalny, co oznacza, że dane, które zostały "zaszyfrowane", można odszyfrować za pomocą odpowiedniego klucza.

RODO

SZERSZY ZAKRES INFORMOWANIA

Obowiązek informacyjny, narzucony na administratora podczas zbierania danych, zostanie znacznie poszerzony.

Będzie trzeba informować o:

- inspektorze ochrony danych,
- nazwie i danych kontaktowych przedstawiciela, jeżeli istnieje,
- podstawie prawnej przetwarzania,
- prawnie uzasadnionym interesie administratora, jeżeli na tej podstawie odbywa się przetwarzanie,
- informacji o zamiarze przekazywania danych do państwa trzeciego,
- okresie, przez który dane osobowe będą przechowywane, bądź kryteria ustalania tego okresu,
- profilowaniu,
- o prawie wniesienia skargi do organu nadzorczego,
- w przypadku istnienia obowiązku podania danych osobowych: wskazaniu ewentualnych konsekwencji
- niepodania danych,

prawach osoby, której dane dotyczą, tj. prawie do:

- usunięcia danych,
- ograniczenia przetwarzania,
- prawie przenoszenia danych,
- prawie do cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych).

RODO

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

- Rozporządzenie zgodę definiuje w art. 4 pkt. 11) i jest nią **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.**

  W polskich przepisach, dotychczasowa definicja brzmiała następująco: to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

ZMIANA: zamiast oświadczenia woli mamy okazanie woli.

Dziękujemy za uwagę!

Centrum Danych Osobowych

www.icdo.pl

797 964 260

biuro@icdo.pl

cdo.icdo