RODO

Najważniejsze zmiany w przepisach o ochronie danych osobowych dla Indywidualnych Praktyk Lekarskich.

1. Podstawowe definicje

- Administrator danych osobowych

Administrator danych osobowych (ADO) to organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. Odnośnie sektora ochrony zdrowia, administratorem danych jest każdy lekarz czy też lekarz dentysta prowadzący indywidualną praktykę. W przypadku innych form prowadzonej działalności leczniczej, administratorem danych jest osoba prawna lub jednostka organizacyjna, np. przychodnia czy szpital (za wyjątkiem sytuacji, kiedy właścicielem przychodni lub szpitala jest osoba fizyczna prowadząca działalność gospodarczą). W związku z tym, iż administratora danych osobowych określa sama ustawa, **wyznaczanie ADO w jakikolwiek sposób, np. poprzez wewnętrze akty prawne (np. zarządzenie lekarza prowadzącego indywidualną praktykę, uchwały organów spółek prawa handlowego) jest niezgodne z przepisami prawa. Funkcji ADO nie można na nikogo cedować.**

Przykłady ADO:

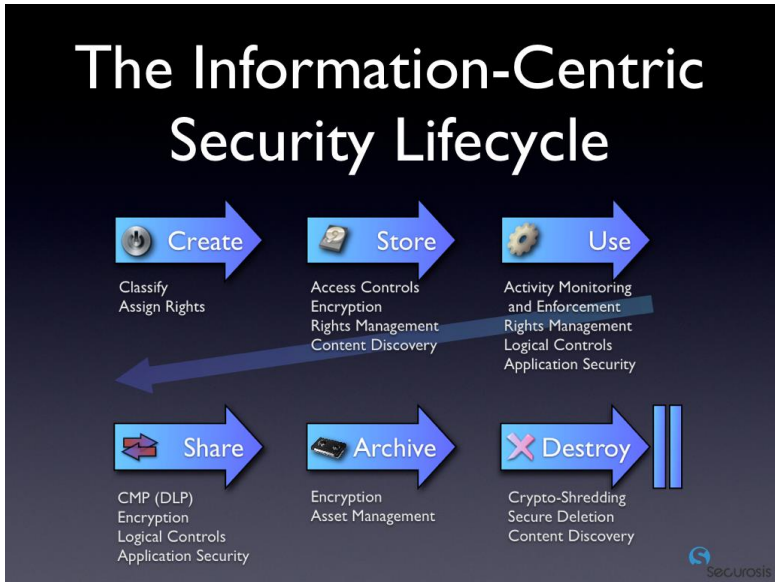
Praktyka zawodowa

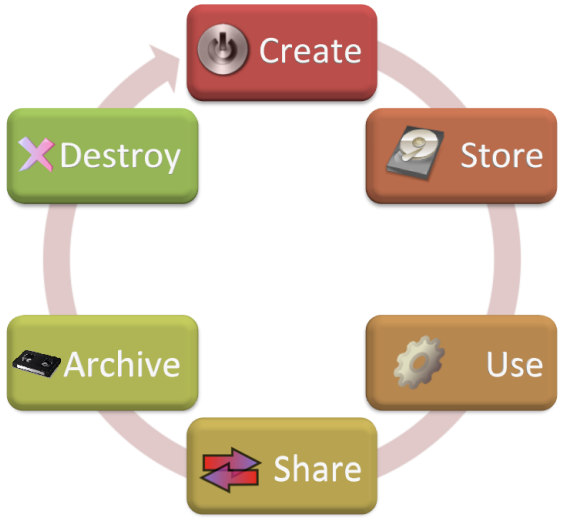
- Praktyka Indywidualna:
  Lekarz prowadzący PI

- Praktyka grupowa:
  Spółka jawna – spółka,
  Spółka partnerska – spółka,
  Spółka cywilna – wspólnicy spółki solidarnie jeśli żaden nie wykona obowiązków RODO, uznaje się za spełnione jeśli obowiązki wykona jeden ze wspólników,

Podmiot leczniczy

- Przedsiębiorca
- Spółka prawa handlowego (osobowa i kapitałowa),
  np,: z o.o., jawna, komandytowa, akcyjna
- SP ZOZ
- Szpital



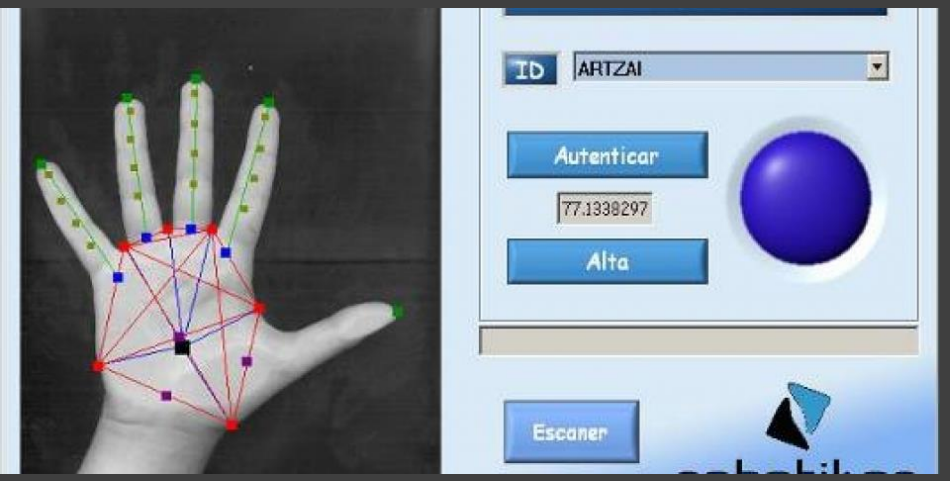


- **Przetwarzanie danych osobowych**

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;

Sposoby przetwarzania – szczegółowe:

- Przegląd/odczyt
- Modyfikacja
- Drukowanie
- Eksport
- Usunięcie
- Transport
- Archiwizacja
- ….



Definicje RODO istotne dla sektora medycznego:

„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 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 dotyczące zdrowia”

oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym (przeszłym, obecnym lub przyszłym) osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

Wrażliwe dane osobowe = Szczególne kategorie danych osobowych

(obecna ustawa) (RODO)

Szczególne kategorie danych osobowych:

- dane genetyczne
- dane biometryczne
- dane dotyczące zdrowia
- pochodzenie rasowe lub etniczne
- Poglądy polityczne
- Przekonania religijne lub światopoglądowe
- Seksualność, orientacja seksualna
- Przynależność do związków zawodowych

2. Nowe obowiązki Administratora danych osobowych.

a) Rozszerzony obowiązek informacyjny i jasnej komunikacji z podmiotami przetwarzania danych osobowych (Pacjenci):

RODO, Art. 6 ust.1 pkt. c – podstawa prawna przetwarzania przez podmiot leczniczy:

(…) Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (…)

Dobra praktyka:

- Informacja umieszczona w widocznych miejscach (np. przy rejestracji, prze drzwiach gabinetów) oraz na stronie internetowej podmiotu.
- Warto pamiętać o klauzulach informacyjnych dla Pracowników.

Co powinna zawierać klauzula informacyjna dla Pacjenta?

Kto będzie przetwarzał moje dane?

W jakim celu?

Jakie są moje prawa?

Czy mam obowiązek podania danych, a jeśli tak to z czego on wynika?

Dane kontaktowe inspektora ochrony danych

Zamiar przekazania danych osobowych do państwa trzeciego

Okres przechowywania danych (ew. przesłanki usunięcia)

Profilowanie

RODO – podejście oparte na ryzyku.

I. Brak gotowych, narzuconych rozwiązań – ADO sam ocenia ryzyko związane z przetwarzaniem danych i dobiera odpowiednie zabezpieczenia, neutralność technologiczna.

II. ADO ma obowiązek rozliczalności – wykazuje organowi nadzorczemu czy dokłada odpowiedniej staranności przy przetwarzaniu danych (np. odpowiednia dokumentacja, zabezpieczenia, kultura organizacyjna, przeprowadzanie oceny skutków dla ochrony danych).

Ocena ryzyka

- Bieżąca;
- Przy ocenie skutków przedsięwzięcia dla ochrony danych (DPIA);
- Przy analizie incydentów naruszenia bezpieczeństwa ochrony danych osobowych - zgłaszanie naruszeń bezpieczeństwa danych osobowych organowi nadzorczemu – ryzyko naruszenia praw i wolności osób, których dane przetwarzamy.

Kiedy wykonujemy DPIA –przykłady:

- Nowe oprogramowanie
- Zakup sprzętu medycznego (dane osobowe, medyczne, genetyczne, biometryczne)
- Monitoring wizyjny
- Umowy z podmiotami zewnętrznymi, zmiany lokalizacji komórek organizacyjnych, np. archiwum, nowe procedury wewnętrzne,

Czy lekarz prowadzący IP ma obowiązek przeprowadzać DPIA? (Motyw 91 RODO)

„Powinno to mieć zastosowanie w szczególności do operacji przetwarzania o dużej skali – które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, na przykład (ze względu na swój szczególny charakter) gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia – oraz do innych operacji przetwarzania powodujących wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności gdy operacje te utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw. Oceny skutków dla ochrony danych należy także dokonywać w przypadkach, w których dane osobowe przetwarza się w celu podjęcia decyzji wobec konkretnej osoby fizycznej po dokonaniu systematycznej, kompleksowej oceny czynników osobowych osób fizycznych na podstawie profilowania tych danych lub po przetworzeniu szczególnych kategorii danych osobowych, danych biometrycznych lub danych osobowych dotyczących wyroków skazujących, naruszeń prawa lub odnośnych 4.5.2016 PL Dziennik Urzędowy Unii Europejskiej L 119/17 środków bezpieczeństwa. Ocena skutków dla ochrony danych jest niezbędna również w przypadku monitorowania na dużą skalę miejsc publicznie dostępnych – w szczególności za pomocą urządzeń optyczno-elektronicznych – lub wszelkich innych operacji, względem których właściwy organ nadzorczy uznaje, że przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności dlatego, że operacje te uniemożliwiają osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy lub mają systematyczny charakter i dużą skalę. Przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika. W takich przypadkach ocena skutków dla ochrony danych nie powinna być obowiązkowa.”

Obowiązki dokumentacyjne.

<u>Pozostaje,</u>

ponieważ RODO wymaga odpowiednich polityk,

procedur opisujących sposób przetwarzania danych:

- Polityka bezpieczeństwa danych osobowych
- Instrukcja zarządzania systemem informatycznym

<u>Dowolność w nazewnictwie</u>

Obowiązki dokumentacyjne.

- Rejestr czynności przetwarzania danych,
- Obowiązek informacyjny
- Procedura zarządzania ryzykiem w podmiocie medycznym
- Rejestr incydentów naruszenia bezpieczeństwa danych osobowych
- Procedura zgłaszania incydentów do organu nadzorczego
- Procedura DPIA
- Umowy powierzenia danych osobowych

3. Kategorie odpowiedzialności Administratora danych osobowych na gruncie RODO i nowej Ustawy o ochronie danych osobowych. Wysokość kar i sposób ich nakładania.

- Wzmocnione zostają prawa jednostki, m.in.:

a. Prawo wglądu i aktualizowania danych,

b. Prawo usunięcia danych (ograniczone przepisami szczegółowymi, np. terminami przechowywania dokumentacji medycznej, pracowniczej)

c. Prawo do przenoszenia danych – tam, gdzie podstawa przetwarzania to umowa,

d. Prawo do ograniczonego przetwarzania,

- Kary administracyjne

Art. 83 ust. 5 Rozporządzenia:

„administracyjna kara pieniężna”

(…) do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa (…)

Podmioty publiczne: 100 000 zł (przepisy krajowe)

- Odpowiedzialność na gruncie przepisów Kodeksu Cywilnego

4.Praktyczne aspekty przetwarzania danych osobowych – przygotowanie do RODO:

a. Inwentaryzacja aktywów informacyjnych;

b. Zabezpieczenia techniczne i organizacyjne (szafy na dokumentację medyczną zamykane na klucz, alarmy przeciwwłamaniowy i ppoż, bezpieczne logowanie do systemu, oświadczenia pracowników, upoważnienia do przetwarzania danych osobowych, polityki ochrony danych osobowych pacjentów i pracowników, inne procedury);

c. Powierzenie przetwarzania danych osobowych – umowy powierzenia przetwarzania danych na gruncie RODO i Ustawy o prawach Pacjenta i Rzeczniku Praw Pacjenta z podmiotami przetwarzającymi – rozszerzone obowiązki Administratora danych;

d. Utylizacja dokumentacji medycznej;

e. Monitoring wizyjny;

f. Udostępnianie dokumentacji medycznej;

g. Bezpieczny e-mail;

h. Szkolenia pracowników;

i. Zmiany w kodeksie pracy;

j. Przetwarzanie danych w celu innym niż leczenie Pacjenta (np. reklama nowych usług) a obowiązki wynikające z RODO.

5. Nowy organ ochrony danych osobowych i sposób prowadzenia przez niego kontroli dotyczącej prawidłowego przetwarzania danych osobowych.

GIODO zostanie zastąpione Urzędem Ochrony Danych Osobowych z Prezesem na czele.

Sposób kontroli regulować będzie nowa Ustawa o ochronie danych osobowych (Rozdział 9 Ustawy):

Kontrolę może przeprowadzić:

- Pracownik UODO
- Pracownik lub członek organu nadzorczego państwa członkowskiego UE
- Postępowanie kontrolne może trwać max.30 dni
- Prezes UODO nie musi uprzednio informować o wszczęciu kontroli, stan ochrony danych może również sprawdzać przy pomocy IOD,
- Kontrola nie wyklucza jednoczesnego lub późniejszego rozpatrywania sprawy (tej lub innej) przez sąd cywilny – np. karę może nałożyć Prezes, a następnie osoba, której dane osobowe niewłaściwie przetwarzano może ubiegać się np. zadośćuczynienia w sądzie cywilnym

6. Inspektor ochrony danych – czy należy go powołać w IP? Jaka jest jego rola i odpowiedzialność? W czym może pomóc Administratorowi danych?

ABI = Inspektor ochrony danych osobowych – funkcja doradcza i weryfikacyjna względem ADO, zatrudniany przez ADO, ale pozostający w bezpośrednim kontakcie z GIODO, quasi-audytor.

Niezależny, podległy bezpośrednio najwyższemu kierownictwu.

Wymagana wiedza fachowa na temat prawa i praktyk w dziedzinie ochrony danych osobowych

Zakaz wydawania instrukcji.

ADO gwarantuje niezależność DPO i odpowiada za to przed organem nadzorczym (kary finansowe mogą być również nałożone za niewłaściwe wykonywanie obowiązków ADO wobec IOD)

DPO stanowić ma punkt kontaktowy dla GIODO i podmiotów ochrony danych (pracowników, pacjentów, kontrahentów, innych interesariuszy).

IOD to osoba fizyczna – konieczne wskazanie konkretnej osoby, a nie np. firmy.

ADO nie może powołać się na IOD.

IOD nie może być żadna osoba, która decyduje o środkach i celach przetwarzania danych osobowych – np. członek zarządu spółki, wspólnik w spółce cywilnej.

Kiedy istnieje obowiązek powołania IOD?

Ogólne rozporządzenie o ochronie danych w art. 37 us.t 1 przewiduje obowiązek wyznaczenia inspektora dla administratorów i podmiotów przetwarzających w następujących przypadkach, gdy:

- przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę.
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych *(dane o stanie zdrowia, biometryczne, genetyczne)*, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10.

Źródło: Puls, luty 2018, nr 2, Miesięcznik OIL w Warszawie im. prof. Jana Nielubowicza (cały artykuł dostępny w Internecie)

Fot. archiwum

Z dr. **Maciejem Kaweckim**, dyrektorem Departamentu Zarządzania Danymi w Ministerstwie Cyfryzacji, rozmawia Ewa Szarkowska.

Nowe regulacje oznaczają dla systemu ochrony zdrowia sporo istotnych zmian, do których trzeba się przygotować.

Sektor zdrowia to obszar, w którym dane osobowe są przetwarzane w ogromnych zasobach. Nie ma innego podmiotu, który by przetwarzał większą liczbę danych dotyczących zdrowia niż NFZ. Poza tym prawie wszystkie gromadzone dane są danymi wrażliwymi, bo dotyczą naszego stanu zdrowia, a zatem szczególnie chronionymi. I dlatego w zasadzie w całości sektor medyczny będzie objęty obowiązkiem powołania inspektora ochrony danych. I nie ma tu znaczenia, czy jest to duży szpital, czy mała praktyka lekarska. Jeśli lekarz przyjmuje dziennie czterech pacjentów, tygodniowo ma ich 20, miesięcznie co najmniej 80, w ciągu roku ponad 1000, a w ciągu paru lat – kilka tysięcy. I jest zobowiązany do powołania inspektora danych osobowych. Obowiązek ten dotyczy również lekarza specjalisty, który w ramach indywidualnej działalności gospodarczej przyjmuje prywatnie tylko raz w miesiącu, a także lekarza, który prowadzi własną praktykę lekarską w pomieszczeniu wynajętym przez szpital. W przypadku kontraktorów, wynajętych jako podwykonawcy przez szpital, odpowiedzialność za zabezpieczenie danych osobowych ponosi ów szpital. Lekarze na kontraktach mają jednak obowiązek stosować się do wdrożonych przez placówkę procedur bezpieczeństwa.

To jest pierwsza zmiana bardzo istotna, odczuwalna i kosztogenna dla sektora medycznego. Nikt nie pracuje za darmo i inspektorowi należy się wynagrodzenie, bo musi opracować i wdrożyć procedury zapewniające bezpieczeństwo zbiorów danych wrażliwych. W dużym szpitalu prawdopodobnie to będzie osoba zatrudniona na etacie. Jednoosobowe praktyki lekarskie zapewne będą korzystały z outsourcingu zewnętrznego podmiotu.