RODO

Zbliża się dzień 25 maja 2018 r. To ważna data dla wszystkich podmiotów leczniczych, praktyk indywidualnych czy też szpitali, ponieważ tego dnia zakończy się okres, w którym była możliwość dostosowania się do przepisów **Rozporządzenia 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) –** tekst dostępny na stronie Generalnego Inspektora Ochrony Danych Osobowych (tutaj)

Jest to zasadnicza zmiana, ponieważ po raz pierwszy w historii problematykę danych osobowych instytucje Unii Europejskiej uregulowały bezpośrednio, co oznacza, że nie będzie krajowych przepisów wykonawczych. Wprawdzie Ministerstwo Cyfryzacji opublikowało we wrześniu ub. roku projekt nowej ustawy jednak jest ona bardzo wąska w swojej treści w porównaniu do obecnych zapisów – tekst projektu dostępny na stronach Ministerstwa Cyfryzacji (tutaj). Jednak do dnia dzisiejszego projekt nie zmienił swojego statusu i wobec wielu uwag zgłoszonych przez wiele podmiotów i instytucji dyskusja trwa nadal, co nie wróży jej szybkiego uchwalenia.

Bez wątpienia każdy, kto prowadzi zarobkową działalność gospodarczą ma de facto do czynienia z danymi osobowymi i staje się ich administratorem. Nie omija to także środowiska lekarzy i lekarzy dentystów, którzy, czy to w ramach praktyki zawodowej, czy też podmiotu leczniczego, świadczą usługi medyczne na rzecz swoich pacjentów i przetwarzają ich dane osobowe. **Obowiązek posiadania dokumentów wewnętrznych jest bezwzględny.**

Poniższa tabela przybliża nieco podstawowe różnice:

Obecne przepisy	**Wymogi RODO**
Polityka bezpieczeństwa	Rejestr czynności przetwarzania
Instrukcja zarządzania systemem informatycznym	Polityka ochrony danych osobowych/ regulamin wewnętrzny
Wyodrębnienie zbiorów w instytucji i wskazanie podstaw prawnych do przetwarzania	Wyodrębnienie zbiorów w instytucji i wskazanie podstaw prawnych do przetwarzania - weryfikacja
Upoważnienia imienne do przetwarzania danych	Upoważnienia imienne do przetwarzania danych
Klauzula informacyjna	Rozszerzenie klauzuli informacyjnej
Zgody na przetwarzanie danych osobowych	Weryfikacja podstaw prawnych zgód na przetwarzanie danych osobowych
Polityka dotycząca incydentów i naruszeń	Procedura dotycząca sposobu powiadamiania UODO o naruszeniach i incydentach
	Procedury zapewnienia ciągłości działania systemu ochrony danych osobowych w jednostce
Rejestracja zbiorów w GIODO	Wewnętrzny rejestr czynności przetwarzania w wersji papierowej i elektronicznej udostępniany na żądanie organu nadzorczego
Konieczność rejestracji ABI w rejestrze GIODO	Poinformowanie UODO o danych kontaktowych DPO
Analiza ryzyka	Analiza ryzyka i ocena skutków ochrony danych

W obecnym porządku prawnym za przestrzeganie przepisów o ochronie danych osobowych odpowiadają tzw. Administratorzy Danych. Nie zmieni się to, ale będzie jednak pewna różnica, ponieważ na dzień dzisiejszy Administrator danych może powołać tzw. Administratorra Bezpieczeństwa Informacji.

Jest to osoba, która odpowiadają za nadzór nad przestrzeganiem przepisów związanych z ochroną danych osobowych w tych podmiotach w imieniu administratora danych osobowych. **Należy w tym miejscu podkreślić, że żadne przepisy nie nakładają na te osoby konieczności posiadania certyfikatów czy też specjalistycznego wykształcenia.** Od takiej osoby wymagane jest jedynie posiadanie stosownej wiedzy. Jednak obowiązek weryfikacji tej wiedzy spoczywa tylko na powierzającym tą funkcję, czyli na administratorze danych, Ale jeśli już powołany zostanie administrator bezpieczeństwa informacji musi on zostać zgłoszony do rejestru prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO). Administrator danych może jednak wykonywać obowiązki nadzorcze osobiście i wtedy nie ma obowiązku zgłaszania tego faktu organowi nadzorczemu tj. GIODO. W nowym porządku prawnym wskazane zostały sytuacje, kiedy Administrator ma obowiązek powołania następcy ABI, czyli Inspektora Ochrony Danych (szczegółowy opis poniżej). Co do zasady obowiązek taki został nałożony na wszystkich administratorów za wyjątkiem pojedynczych lekarzy i lekarzy dentystów, którzy prowadzą indywidualne praktyki. Może jednak uda się rozszerzyć nieco to wyłączenie z obowiązku powołania takich inspektorów, ale prace wciąż trwają i niestety nie jest to przesądzone.

Bardzo ważnym elementem nowego podejścia do problematyki ochrony danych osobowych jest położenie nacisku w nowym rozporządzeniu na zapobieganie i szacowanie ryzyka procesu przetwarzania danych osobowych. Stąd każdy administrator będzie musiał wykazać się w tym zakresie opisem czynności przetwarzania danych osobowych w odniesieniu do zagrożeń procesów. I tak pojedynczy lekarze w praktykach lekarskich będą mogli poprzestać na takiej analizie ryzyka, a większe podmioty będą musiały po 25 maja przeprowadzać tzw. ocenę skutków dla ochrony danych, o której mówi art. 35 RODO. Szczegółowo ta tematyka omówiona jest niżej.

Wspominano wcześniej, że RODO obowiązuje bezpośrednio w państwach członkowskich, co oznacza, że nie będzie polskich aktów wykonawczych, które wskazywałyby drogę administratorom jak wykazać się stosowaniem procedur RODO. Pomocne mają być tzw. kodeksy branżowe. W chwili obecnej trwają prace nad takim branżowym kodeksem dla sektora ochrony zdrowia, w których to pracach uczestniczy również Wielkopolska Izba Lekarska, ale jest to również proces, który zakończy się bliżej maja br. To w tym akcie będą kierunki i wskazówki, dzięki którym będzie możliwość skorzystania z pewnych rozwiązań. Nowe przepisy przewidują również mechanizmy certyfikacji i akredytacji, które będą funkcjonować na podobnych zasadach jak obowiązujące w ochronie zdrowia procedury jakościowe.

Rozporządzenie o ochronie danych osobowych przyniesie również zmianę nazwy organu nadzorczego z GIODO na prawdopodobnie Urząd Ochrony Danych Osobowych. Trzeba w tym miejscu dodać, że ma to być silna instytucja, która będzie miała odpowiednie narzędzia do działania oraz będzie dysponować szerokim dostępem do sankcji:

Kary do 10 mln. EUR lub do 2 % jego całkowitego rocznego światowego obrotu za naruszenia w zakresie: rejestrowania czynności przetwarzania, współadministrowania, współpracy z UODO oraz z podmiotem przetwarzającym, upoważniania, wdrożenia zabezpieczeń, zgłaszania naruszeń, oceny skutków, pracy IOD

Kary do 20 mln. EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu za naruszenia w zakresie: legalności przetwarzania, warunków zgód, celowości, adekwatności, czasowości, obowiązku informacyjnego, praw osób, niezgodnego z prawem przetwarzania oraz ochrony przed utratą, zniszczeniem lub uszkodzeniem danych

Kary do 100.000 PLN dla podmiotów publicznych

Przepisy rozporządzenia są również znaczące z kilku innych perspektyw, ponieważ w sposób bezpośredni odnoszą się do postępujących procesów technologicznych i informatycznych. Dynamiczny rozwój sieci internetowej, wymiany informacji i usług społeczeństwa informacyjnego wymaga interwencji w zakresie ochrony danych osobowych i stąd nowe terminy w tym obszarze jak anonimizacja danych, prawo do bycia zapomnianym czy ograniczenia w zakresie tzw. profilowania. Jednak rozwijanie tych pojęć to raczej materiał na oddzielne omówienie.

mgr Marek Saj

Trwają prace nad kodeksem branżowym dla lekarzy/lekarzy dentystów, który będzie niezmiernie istotnym dokumentem doprecyzowującym tą materię wobec tego radzimy zachować powściągliwość w zakresie nawiązywania współpracy z zewnętrznymi firmami. Wkrótce zostanie ustalony termin szkolenia w/w zakresie, które odbędzie się w biurze Bydgoskiej Izby Lekarskiej.