RODO w praktykach zawodowych lekarzy i lekarzy dentystów

Wejście w życie.

Rozporządzenie Parlamentu Europejskiego i Rady 2016/679 – nazywane potocznie RODO – wejdzie w życie na terenie Rzeczypospolitej Polskiej i pozostałych państw członkowskich Unii Europejskiej z dniem 25 maja 2018 r. Od tego dnia wszystkie podmioty przetwarzające dane osobowe, w tym lekarze i lekarze dentyści prowadzący praktyki zawodowe i podmioty lecznicze, będą zobowiązane do jego stosowania (wyjątek stanowią jedynie praktyki kontraktowe, które nie mają statusu administratora danych osobowych). Obecnie na etapie legislacyjnym jest również projekt nowej ustawy o ochronie danych osobowych oraz przepisów wprowadzających do niej. Celem ustawy będzie jednak jedynie uszczegółowienie przepisów RODO oraz ewentualna odmienna regulacja krajowa – tam gdzie RODO na to pozwala.

Szerszy obowiązek informacyjny.

Rozporządzenie przewiduje rozszerzenie obowiązku informacyjnego przy zbieraniu i przechowywaniu wszelkich danych osobowych, w tym obowiązek podawania osobom, których dane dotyczą m.in.:

- danych administratora i ewentualnego inspektora ochrony danych osobowych, w tym danych kontaktowych;
- celu przetwarzania danych i kategoriach przetwarzanych danych;
- informacji o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- informacji o ewentualnym zamiarze przekazania danych osobowych do państwa trzeciego (np. na serwery poza terenem Unii Europejskiej);
- okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacji o prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także o prawie do przenoszenia danych;
- informacji o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (w takim wypadku co do zasady dane osobowe pacjentów będą przetwarzane na podstawie obowiązujących przepisów, a nie zgody pacjenta);
- informacji o prawie wniesienia skargi do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych);
- informacji, jakie są ewentualne konsekwencje niepodania danych osobowych;

Wejście w życie rozporządzenia będzie się zatem wiązało z koniecznością uzupełnienia dotychczasowych zgód na przetwarzanie danych osobowych, jeżeli są stosowane, szerszą informacją o przetwarzaniu danych osobowych zarówno na etapie zbierania danych od pacjentów (np. w ramach rejestracji), jak również na etapie późniejszego przetwarzania tych danych.

Koniec rejestru zbiorów danych osobowych.

Projekt nowej ustawy o ochronie danych osobowych przewiduje całkowitą rezygnację z obowiązku rejestracji zbiorów danych osobowych, które w bardzo niewielkim stopniu

dotyczyły dotychczas działalności medycznej – z uwagi na ustawowe zwolnienie zbiorów danych osób korzystających z usług medycznych.

Szersze umowy o powierzenie przetwarzania danych.

Dotychczasowa ustawa o ochronie danych osobowych przewidywała jedynie, że umowa o powierzenie przetwarzania danych ma być zawarta w formie pisemnej, bez szczegółowego określania jej treści. RODO przewiduje natomiast szczegółową treść wskazanej umowy. W związku z powyższym **konieczne będzie aneksowanie dotychczasowych umów o powierzenie przetwarzania danych, które lekarze i lekarze dentyści zawarli z podmiotami przetwarzającymi (np. firmami serwisującymi sprzęt medyczny przechowujący dane o badaniach, producentami oprogramowania do prowadzenia gabinetów, firmami informatycznymi, zewnętrznymi firmami księgowymi i kadrowymi itp.), w celu ich dostosowania do nowych wymogów.**

Inspektor ochrony danych osobowych (IODO).

Obecnie obowiązujące przepisy przewidują, że powoływanie administratora bezpieczeństwa informacji jest dobrowolne i zależy wyłącznie od decyzji danego przedsiębiorcy. RODO wprowadza natomiast obowiązek powołania IODO w każdym przypadku, gdy główna działalność administratora polega na przetwarzaniu na dużą skalę danych wrażliwych, w tym danych o zdrowiu. **W świetle prac grupy roboczej działającej przy Generalnym Inspektorze Danych Osobowych z obowiązku powoływania inspektorów mają być zwolnione indywidualne praktyki lekarskie.** Z uwagi na niezakończenie prac legislacyjnych nad ustawą nie jest możliwe obecnie jednoznaczne ustalenie, czy taka rekomendacja wejdzie w życie. Również RODO wskazuje, iż obowiązek powołania inspektora nie będzie co do zasady dotyczył administratora będącego pojedynczym lekarzem. **Na obecnym etapie można natomiast wstępnie założyć, że obowiązek powołania inspektorów będzie dotyczył wszystkich podmiotów leczniczych.** Dyskusyjna może być jedynie kwestia działania inspektorów w małych podmiotach (jedno- lub dwuosobowych) oraz w grupowych praktykach lekarskich. Inspektorem może być zarówno pracownik, jak i podmiot zewnętrzny w stosunku do przedsiębiorcy. Nie może być nim jedynie sam administrator z uwagi na konieczność zachowania niezależności IODO. RODO nie wprowadza jednak żadnych szczególnych wymogów kwalifikacyjnych dla osoby sprawującej taką funkcję, poza wskazaniem, iż musi ona posiadać wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych.

Nowa dokumentacja.

Nowa ustawa nie przewiduje już konieczności opracowywania polityki bezpieczeństwa w zakresie danych osobowych oraz instrukcji bezpieczeństwa systemu informatycznego. Zamiast tych dokumentów RODO wprowadza jednak obowiązek posiadania przez wszystkie podmioty przetwarzające szczególne kategorie danych (tzw. dane wrażliwe) nowego dokumentu – rejestru czynności przetwarzania. Będzie on zawierał m.in. informacje o technicznych i organizacyjnych środków bezpieczeństwa. Podstawą jego opracowania powinna być w znacznej mierze istniejąca u Państwa polityka bezpieczeństwa i instrukcja.

Obowiązek zgłaszania naruszeń.

Projekt ustawy o ochronie danych osobowych przewiduje obowiązek dokonywania przez

elektronicznych zgłoszeń do Prezesa Urzędu Ochrony Danych Osobowych w wypadku naruszenia bezpieczeństwa danych. Zgłoszenia te miałyby być dokonywane bez zbędnej zwłoki, nie później niż **w terminie 72 godzin po stwierdzeniu naruszenia. Dodatkowo konieczne będzie prowadzenie dokumentacji stwierdzonych naruszeń oraz informowanie osób, których dane dotyczą o naruszeniach, które wystąpiły (poprzez informację indywidualną albo publiczny komunikat).**

Administracyjne kary pieniężne.

RODO przewiduje wysokie kary administracyjne za naruszenia dotyczące przetwarzania danych osobowych. Górna granica kar to aż 20.000 000 EUR lub do 4 % całkowitego rocznego obrotu. Należy jednak pamiętać, że RODO zawiera również przesłanki, jakimi powinien kierować się Prezes Urzędu wymierzając karę pieniężną. Niemniej jednak, dolegliwość finansowa powinna być jednym z czynników motywujących lekarzy i lekarzy dentystów do zapoznania się z regulacjami RODO i wdrożenia ich w swoich praktykach.

Wdrażanie RODO.

Przed przystąpieniem do przetwarzania danych osobowych na nowych zasadach podmiot przetwarzający dane wrażliwe powinien co do zasady przeprowadzić analizę ryzyka (poprzez stworzenie dokumentu oceny skutków dla ochrony danych). Z obowiązku jego sporządzania nie będą zwolnieni przedsiębiorcy, którzy przetwarzają na dużą skalę owe dane. Istnieje zatem szansa, że podobnie jak w odniesieniu do obowiązku powołania IODO, indywidualne praktyki będą z tej analizy ryzyka zwolnione.

Akty prawne.

- 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
- Projekt ustawy o ochronie danych osobowych z dnia 8 lutego 2018 r.
- Projekt ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych z dnia 14 września 2017 r.

adw. Damian Konieczny
Instytut – Specjaliści Prawa Ochrony Zdrowia
www.ispoz.pl