Co w RODO piszczy?

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), zwane dalej RODO, będzie obowiązywało w polskim porządku prawnym bezpośrednio i będzie miało zastosowanie od dnia 25 maja 2018 r. Z tym dniem wszystkie podmioty przetwarzające dane osobowe, będą zobowiązane do jego stosowania. Dotyczy to także lekarzy i lekarzy dentystów prowadzących praktyki zawodowe i podmioty lecznicze. Dopiero w dniu 5 kwietnia br. wpłynął do Sejmu RP, rządowy projekt nowej ustawy o ochronie danych osobowych, której celem jest uszczegółowienie przepisów RODO i tam gdzie dopuszcza to regulacja unijna, szczególna regulacja krajowa.

Najważniejsze zmiany wynikające z nowych przepisów:

1. Likwidacja rejestrów zbiorów danych osobowych.

Projekt nowej ustawy o ochronie danych osobowych przewiduje likwidację obowiązku rejestracji zbiorów danych osobowych. Dotychczas w przypadku działalności w zakresie ochrony zdrowia istniało ustawowe zwolnienie z obowiązku rejestracji zbiorów danych pacjentów.

2. Zastąpienie Administratora bezpieczeństwa informacji (ABI), Inspektorem ochrony danych osobowych (IODO).

Dotychczasowe przepisy przewidują, iż powołanie ABI jest czynnością fakultatywną i zależy wyłącznie od decyzji administratora danych. RODO wprowadza natomiast obowiązek powołania IODO w każdym przypadku, gdy główna działalność polega na przetwarzaniu na dużą skalę danych wrażliwych, również co do stanu zdrowia. Projekty regulacji krajowych przewidują, iż z obowiązku powoływania IODO mają być zwolnione m.in. indywidualne i grupowe praktyki lekarskie, o ile nie prowadzą działalności na dużą skalę. W chwili obecnej, ze względu na trwający proces legislacyjny, nie jest pewne czy rozwiązanie takie zostanie w jakiś sposób ograniczone, w szczególności ze względu na określenie skali działalności.

3. Rozszerzenie obowiązku informacyjnego.

RODO przewiduje rozszerzenie obowiązku informacyjnego przy zbieraniu i przechowywaniu danych osobowych, w tym w szczególności podanie:
- danych administratora i ewentualnego inspektora ochrony danych osobowych, w tym danych kontaktowych;
- celu przetwarzania danych i ich kategoriach;
- informacji o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- informacji o ewentualnym zamiarze przekazania danych osobowych do państwa trzeciego;
- 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;
- informacji o prawie wniesienia skargi do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych);
- informacji, jakie są ewentualne konsekwencje niepodania danych osobowy, przykładowo co do odmowy udzielenia świadczenia.

4. Zmiana treści umów, w przypadku gdy przewidują one przetwarzanie danych osobowych przez inne podmioty.

W przypadku umów zawartych przez lekarzy w ramach prowadzonej działalności leczniczej, przykładowo w zakresie badań diagnostycznych, serwisowania sprzętu, czy infrastruktury informatycznej, będą one wymagały uzupełnienia w zakresie upoważnienia do przetwarzania danych osobowych, zgodnie z wymaganiami RODO. W chwili obecnej większość profesjonalnych firm, przesyła do lekarzy stosowne aneksy, w celu wypełnienia tego obowiązku.

5. Nowe regulacje wewnętrzne.

Nowe przepisy nie przewidują już konieczności opracowywania polityki bezpieczeństwa danych osobowych oraz instrukcji bezpieczeństwa systemu informatycznego. W zamian RODO wprowadza, obowiązek opracowania przez wszystkie podmioty przetwarzające dane wrażliwe nowego dokumentu – Rejestru czynności przetwarzania, który zawierać ma informacje o technicznych i organizacyjnych środkach bezpieczeństwa.

6. Nowy obowiązek zgłaszania naruszeń.
Regulacja wprowadza obowiązek dokonywania elektronicznych zgłoszeń Prezesowi Urzędu Ochrony Danych Osobowych przypadków naruszenia bezpieczeństwa danych. Mają być one dokonywane bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wprowadzony będzie obowiązek dokumentowania stwierdzonych naruszeń oraz nakaz informowania osób, których to dotyczy, o mających miejsce naruszeniach, przez informację indywidualną albo publiczny komunikat.

7. Wysokie kary pieniężne.

Za naruszenie nowych przepisów dotyczących przetwarzania danych osobowych, przewidziano surowe kary pieniężne, które mogą wynieść aż równowartość 20 000 000 EURO lub do 4 % całkowitego rocznego obrotu.
Podsumowanie
Wskazana powyżej wysokość kar, która może być nałożona na podmioty naruszające RODO, powinna skłonić wszystkich, w tym również lekarzy udzielających świadczeń zdrowotnych w ramach praktyk, do podjęcia działań przygotowujących do wdrożenia nowych regulacji. W chwili obecnej, ze względu na trwające dalej prace legislacyjne, istnieje jednak trudność we wskazaniu szczegółowych wymogów, które muszą spełniać praktyki lekarskie. Dotyczy to przykładowo obowiązku przeprowadzenia analizy istniejącego ryzyka ochrony danych osobowych, gdyż przewiduje się, że podmioty prowadzące działalność na małą skalę (w tym praktyki lekarskie), będą z tego obowiązku zwolnione.
Należy jednak pamiętać, że wszystkie podmioty, w tym również działalności leczniczej, które przetwarzają dane szczególnie wrażliwe na dużą skalę, będą musiały spełnić wszystkie wymagania przewidziane przez nowe regulacje.