Obowiązki podmiotów medycznych

Nadal wiele znaków zapytania. W ostatnim czasie coraz głośniej mówi się o Rozporządzeniu Parlamentu Europejskiego i Rady UE nr 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 (w skrócie RODO). Nie dzieje się to bez przyczyny, ponieważ począwszy od 25 maja 2018 r. RODO dość znacznie przemodeluje sposób, w jaki wykorzystujemy dane osobowe.

O tym, iż istnieje polska ustawa o ochronie danych osobowych wie prawie każdy i prawdopodobnie każdy też ma świadomość, jak do tej pory była przestrzegana przez różne podmioty. Można więc przyjąć z dużą dozą prawdopodobieństwa, że powszechnie nie zwrócono by większej uwagi na kolejne „Rozporządzenie Unijne" w tym zakresie, gdyby nie to, że: po pierwsze - RODO nakłada drakońskie kary za nieprzestrzeganie zasad w nich określonych, a po drugie - wprowadza obowiązki, które dla zwykłego człowieka mogą się wydawać podobnie absurdalne, jak odrębnie regulowana... krzywizna ogórka polnego.

Co się więc zmienia w dniu 25 maja 2018 r. i ile mamy następnie czasu na przygotowania do tych zmian?

Pierwsza zła wiadomość jest taka, że przepisy Rozporządzenia już weszły w życie, co miało miejsce 17 maja 2016 r. i obecnie kończy się nam właśnie czas na dostosowanie się do nowych regulacji - data 25 maja 2018 jest datą graniczną. Drugą informacją jest ta, że nasz parlament - oczywiście - na ostatnią chwilę stara się uchwalić nową ustawę o ochronie danych osobowych, która będzie uwzględniała wszystkie regulacje zawarte w RODO oraz przygotować przepisy wykonawcze do tej ustawy. Nie jest to jednak wiadomość dobra - świadcząca o tym, że mamy więcej czasu na dostosowanie się do nowych przepisów. RODO jest bowiem tego typu aktem prawa UE, które jest stosowane w krajach unijnych, w tym w Polsce bezpośrednio - nawet bez przepisów polskich i pomimo, iż przepisy polskiego prawa będą z nim sprzeczne.

Jak się zatem najlepiej przygotować do nieuchronnie nadchodzących zmian?

Z pewnością - moim zdaniem - niezbędnym okaże się audyt prawnika lub co najmniej firmy wyspecjalizowanej we wdrożeniach zasad ochrony danych osobowych. Nie sposób

bowiem na łamach krótkiego artykułu w całości i szczegółowo opisać szeregu zmian, jakie są zobowiązane wdrożyć wszystkie podmioty medyczne. A i wdrożenie poszczególnych rozwiązań jest kwestią zbyt indywidualnych potrzeb takich podmiotów, aby możliwe i prawidłowe było ich jedynie ogólne opisanie.

Dlatego też chcę w tym artykule przede wszystkim zwrócić uwagę na fakt, że każdy podmiot świadczący usługi medyczne przetwarza najbardziej wrażliwe i najbardziej chronione dane osobowe. To zaś bezwzględnie wiąże się z koniecznością przestrzegania przepisów Rozporządzenia UE ws. RODO i przystosowania swoich placówek nie tylko do nowych obowiązków biurokratycznych, ale również do przeorganizowania sposobu ich funkcjonowania.

W ramach obowiązków biurokratycznych, ciążących na podmiotach udzielających świadczeń zdrowotnych, można wymienić chociażby obowiązek prowadzenia rejestru przetwarzania czynności danych osobowych. Wspomniany rejestr powinien zawierać szczegółowe zapisy dotyczące (art. 30 RODO):

- danych kontaktowych administratora danych,
- celu przetwarzania danych osobowych,
- opisu kategorii osób, których dane dotyczą oraz zakresu danych,
- kategorii odbiorców, którym dane zostały lub zostaną udostępnione,
- informacji o przekazywaniu danych do państwa trzeciego wraz z dokumentacją opisującą zastosowane zabezpieczenia w tym procesie,
- planowanego terminu usunięcia danych osobowych,
- ogólnego opisu zastosowanych zabezpieczeń technicznych i organizacyjnych.

Innym obowiązkiem, nałożonym na placówki medyczne (art. 28 ust. 3 RODO), jest obowiązek podpisania umów na przetwarzanie danych osobowych ze wszystkimi podmiotami współpracującymi (np. laboratoriami - jeśli przekazane próbki identyfikowane są np. po numerze PESEL, a nie np. po kodzie kreskowym), którym powierza się przetwarzanie danych osobowych pacjentów.

Dodatkowo każdy podmiot medyczny będzie zobowiązany do kierowania klauzul informacyjnych do pacjentów (art. 13 RODO). Treść takich klauzul, zgodnie z przepisami, musi obejmować:

- tożsamość przetwarzającego dane i jego dane kontaktowe, dane kontaktowe inspektora ochrony danych (jeśli został powołany);
- cele przetwarzania danych osobowych i podstawę prawną ich przetwarzania;
- prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony, czy wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

Co prawda ustawodawca unijny nie określił formy przekazywania opisanych wyżej informacji, jednak zaleca się, aby były one przekazywane pisemnie, choć praktyka może dopuścić do sytuacji, w której wystarczające będzie wywieszenie stosownych informacji w widocznym miejscu placówki (np. przy rejestracji). Podmioty udzielające świadczeń zdrowotnych powinny odebrać klauzule informacyjne co najmniej od bieżących pacjentów (brak jest na tę chwilę konieczności poinformowania pacjentów, którzy mają założone karty lecz nie kontynuują leczenia).

Jeśli chodzi o nowe obowiązki związane ze zmianą funkcjonowania sposobu udzielania usług medycznych, to można do nich zaliczyć takie, jak:

- konieczność powierzenia konkretnej osobie obowiązków Inspektora Ochrony Danych,
- realne wprowadzenie zasady tzw. czystego biurka (na biurku pracownika/lekarza nie powinny znajdować się dokumenty więcej niż jednego aktualnie obsługiwanego pacjenta),
- prowadzenie rejestru incydentów, w których mogło bądź doszło do ujawnienia przetwarzanych danych osobowych,
- przygotowanie i wdrożenie polityki bezpieczeństwa i ochrony danych (w tym między innymi zabezpieczenie komputerów przed nieuprawnionym użyciem, zapewnienie każdemu pracownikowi korzystającemu z komputera osobnego konta użytkownika, tak aby możliwe było ustalenie, który z nich miał dostęp do przetwarzanych danych, jakich danych i kiedy, na szczególną uwagę zasługuje zasadność wdrożenia normy ISO 27001),
- przeprowadzenie analizy ryzyka lub oceny skutków dla ochrony danych, szkolenia pracowników.

W gąszczu przepisów oraz niejasności może pracownikom ochrony zdrowia pomóc Kodeks Dobrych Praktyk Dla Ochrony Zdrowia, który chociaż jest inicjatywą oddolną, to jest przygotowywany przez ekspertów z dziedziny prawa i medycyny i który po ostatnich konsultacjach ma zostać niebawem upowszechniony i oddany do użytku dla wszystkich zainteresowanych podmiotów. Polecam zapoznanie się z z tą publikacją.

Aleksandra Granosik - Kaczanowska
radca prawny