

## Sektor medyczny musi wzmocnić ochronę danych osobowych

Już od 20 lat w Polsce obowiązują przepisy o ochronie danych osobowych, dzięki którym dostosowaliśmy nasz system prawny w tym zakresie do standardów obowiązujących w Unii Europejskiej. Oznacza to, że od 20 lat wszyscy administratorzy danych, czyli podmioty decydujące o celach i środkach przetwarzania danych osobowych, a więc również placówki ochrony zdrowia czy przedsiębiorcy prowadzący działalność leczniczą, muszą znać i stosować przepisy o ochronie danych osobowych, które zaimplementowały dyrektywę unijną 94/46/WE.

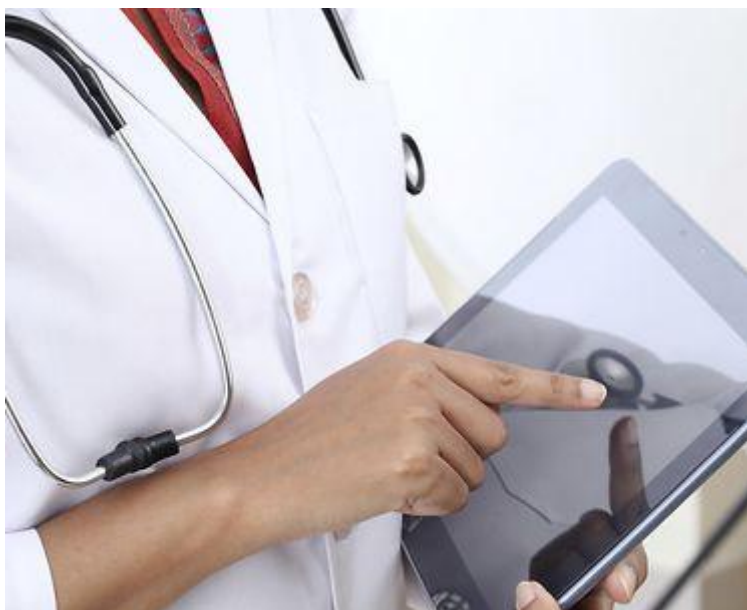


03-11-2017

### GRC Zarządzanie RODO

Warto wiedzieć: Przez wiele lat pacjenci w skargach kierowanych do administratorów danych oraz do Generalnego Inspektora Ochrony Danych Osobowych, zwyczajnie panujące w placówkach opieki zdrowotnej opisywali jako niezgodne z przepisami o ochronie danych osobowych.

Dla menedżerów



Mimo tego – jak wynika z kontroli przeprowadzonych przez GODO w placówkach medycznych oraz wpływającej do urzędu korespondencji, w tym skarg od obywateli – problematyka ta przez wiele lat była konsekwentnie „odstawiana na bocznice”. Placówki opieki zdrowotnej, koncentrując się na świadczeniu usług medycznych, zapominały, że przetwarzają wiele i to najwrażliwszych danych osobowych, które powinny być chronione w sposób szczególny. Panowało błędne przekonanie, iż dla ochrony informacji pozostających w ich zasobach wystarczające jest stosowanie wyłącznie tajemnic zawodowych.

**Na pytania odpowiada Monika Krasieńska, dyrektor Departamentu Orzecznictwa, Legislacji i Skarg w Biurze Generalnego Inspektora Ochrony Danych Osobowych (GODO)**

#### **Czy ochrona danych osobowych dotyczy tylko systemów informatycznych?**

GODO od wielu lat wskazuje na konieczność dostosowania przez sektor ochrony zdrowia zarówno systemów informatycznych, jak i rozwiązań z zakresu organizacji pracy do zasad ochrony danych osobowych. Stworzenie optymalnego systemu ochrony danych osobowych nie polega wyłącznie na opracowaniu dokumentacji opisującej sposób postępowania z danymi osobowymi. Niezwykle istotne jest to, aby udokumentowane zasady realizacji obowiązków administratora danych i jego pracowników zostały wdrożone i stosowane w praktyce. Konieczny jest także stały monitoring przyjętych rozwiązań technicznych i organizacyjnych pod kątem ich aktualności i adekwatności. Pamiętać bowiem należy, iż przetwarzanie danych osobowych następuje nie tylko w systemach informatycznych. Przemodelowania wymaga często – ze względu na ryzyko ujawnienia danych wrażliwych osobom trzecim – nie tylko sposób realizacji pracy przy obsłudze pacjentów, ale także proces ich rejestracji, świadczenie określonych usług medycznych, a nawet proces archiwizacji dokumentacji.

Przez wiele lat sami pacjenci w skargach kierowanych zarówno do administratorów danych, jak i do Generalnego Inspektora Ochrony Danych Osobowych, zwyczajnie panujące w placówkach opieki zdrowotnej opisywali jako niezgodne z przepisami o ochronie danych osobowych. Takie przypadki zdarzają się do dziś i dotyczą na przykład sposobu postępowania z danymi osobowymi w punktach rejestracji pacjentów, gdzie bardzo często, mimo pobierania

od pacjentów dokumentów ich tożsamości do wglądu, dane tych osób i tak są ujawniane osobom nieuprawnionym poprzez głośne odczytywanie nazwisk, numerów PESEL i adresów zamieszkania. Spotykaną wciąż praktyką jest także wywoływanie pacjentów oczekujących na wizytę do lekarza o konkretnej specjalizacji po nazwiskach, co pozwala pośrednio zapoznać się wszystkim osobom postronnym z rodzajem schorzenia pacjenta. Takie same ryzyka powstają przy wywieszaniu list osób zapisanych do danego lekarza np. na drzwiach gabinetów lekarskich czy też umieszczaniu imienia i nazwiska na łóżkach pacjentów znajdujących się na konkretnych oddziałach szpitalnych. Bezrefleksyjne telefoniczne udostępnianie danych o stanie zdrowia pacjenta czy też danych zawartych w dokumentacji medycznej może także prowadzić do zarzutu naruszenia tajemnicy lekarskiej czy pielęgniarskiej.

### **Sygnały takie były wielokrotnie przyczynkiem kierowania przez GODO do kierownictwa placówek wystąpienia z wnioskami o zmianę kwestionowanych praktyk.**

Czasu na dokonanie przez placówki opieki zdrowotnej niezbędnych zmian w obszarze ochrony danych osobowych jest coraz mniej, zważywszy na fakt, że wkrótce niezbędne będzie stosowanie nowych unijnych regulacji, a mianowicie tzw. ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (RODO). Wymuszają one wdrożenie nowych rozwiązań dedykowanych ochronie danych osobowych, a ich brak będzie mógł skutkować nie tylko, jak dotychczas, sankcjami administracyjnymi, ale także finansowymi.

### **Co w związku z tym będą musiały zrobić placówki medyczne?**

Rozpoczęcie stosowania - od 25 maja 2018 roku - unijnego ogólnego rozporządzenia o ochronie danych osobowych, z jednej strony wzmacnia prawa osób, których dane są przetwarzane, z drugiej zaś zwiększa zakres obowiązków administratorów i przetwarzających dane, a tym samym zakres ich odpowiedzialności za przetwarzanie niezgodne z prawem. Perspektywa zbliżającego się rozpoczęcia stosowania przepisów RODO to doskonała okazja na dokonanie przeglądu obowiązującego w danej placówce systemu ochrony danych osobowych. To czas na analizę istniejących luk, a także przyjętych dotychczas rozwiązań pod kątem spełniania nowych wymogów w zakresie ochrony danych osobowych i prywatności. Dodatkowo trzeba pamiętać, że świadcząc usługi medyczne, pod uwagę należy brać nie tylko ogólne przepisy dotyczące ochrony danych osobowych, ale także regulacje sektorowe odnoszące się do godności i ochrony praw pacjenta. Stanowią one dodatkowy bufor chroniący interesy pacjentów i brak ich znajomości będzie prowadził także do naruszenia praw podmiotów danych.

Te placówki, które wprowadziły już określone rozwiązania, muszą teraz sprawdzić, czy spełniają one wszystkie zasady wynikające z ogólnego rozporządzenia o ochronie danych.

Po pierwsze – czy mają podstawę prawną do pozyskiwania i wykorzystywania danych osobowych pacjentów, ich rodzin, pracowników czy kontrahentów. Po drugie - czy spełniają obowiązek informacyjny, podając wszystkie wymagane prawem informacje oraz czy robią to w sposób odpowiednio prosty, przystępny. Pozyskiwane i dalej przetwarzane dane muszą być poddane testowi proporcjonalności. Przeanalizować trzeba także kwestie związane z przekazywaniem przez świadczeniodawców danych osobowych w ramach umów cywilnoprawnych, zawieranych m.in. w związku z prowadzeniem przez podmioty zewnętrzne np. obsługi informatycznej, archiwizacyjnej, rachunkowo-księgowej i itp. Wymagane byłoby w

tym przypadku uwzględnienie przepisów dotyczących powierzenia przetwarzania danych osobowych. Istotne jest także dokonanie przeglądu ewentualnych podstaw prawnych dla udostępniania danych osobowych, w tym wrażliwych, do państw trzecich.

Jeśli chodzi o podstawę prawną uprawniającą placówki medyczne do przetwarzania danych osobowych pacjentów, to najczęściej jest ona określona w szczegółowych przepisach sektorowych. Zaakcentowania przy tym wymaga, iż przepisy te także muszą być dostosowane do RODO, gdyż w przeciwnym przypadku każda osoba, na podstawie RODO jako aktu stosowanego bezpośrednio, będzie mogła dochodzić swych praw i żądać określonych sankcji przed organem nadzorczym. Gdy administrator danych zechce posiłkować się zgodą pacjenta na przetwarzanie danych osobowych, to musi wykazać, iż była ona wyraźna, dobrowolna i spełnia wszystkie warunki, o których mowa w rozporządzeniu, w tym że może być w każdym czasie odwołana, o czym pacjent uprzednio powinien być poinformowany. Dodatkowo, przepisy RODO wyposażają osoby, których dane są przetwarzane, w wiele nowych uprawnień, do realizacji których powinni być przygotowani wszyscy świadczeniodawcy usług leczniczych z sektora publicznego i prywatnego. Do praw tych należą m.in.: prawo do usunięcia danych, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych czy też prawo do kopii danych. Szczególne obowiązki spoczną na podmiotach, które będą przetwarzać dane i podejmować indywidualne decyzje wyłącznie na podstawie zautomatyzowanego przetwarzania, w tym profilowania. Obserwując dynamiczny rozwój technologii w sektorze zdrowia, nie sposób tych nowych praw i obowiązków nie uwzględnić już na etapie projektowania określonych produktów i usług dedykowanych temu sektorowi.

Jedną z naczelných zasad RODO jest zasada rozliczalności, która oznacza, iż każdy administrator jest nie tylko odpowiedzialny za przestrzeganie wszystkich przepisów o ochronie danych osobowych, ale także musi być w stanie wykazać ich przestrzeganie zarówno wobec organu nadzorczego, osób, których dane przetwarza, jak i ogółu społeczeństwa. To duże zmiany.

### **Czy środowisko medyczne zdaje sobie z tego sprawę?**

Na szczęście w ostatnim czasie w szeroko rozumianym sektorze ochrony zdrowia zauważamy postęp w pracach nad umieszczeniem zasad ochrony danych osobowych jako integralnej części prowadzonej działalności leczniczej i świadczonych usług medycznych. Temat ten jest przedmiotem szczególnej uwagi samorządów lekarskich i pielęgniarskich, a także innych środowisk branży medycznej. Generalny Inspektor Ochrony Danych Osobowych pozostaje z nimi w ścisłym kontakcie.

Co ważne, środowiska medyczne widzą potrzebę stworzenia kodeksów postępowania, czyli skorzystania z bardzo korzystnego instrumentu, który przewiduje rozporządzenie o ochronie danych osobowych. Stosowanie takich kodeksów może pomóc we właściwym stosowaniu przepisów o ochronie danych przez dany sektor, z uwzględnieniem jego specyfiki oraz szczególnych potrzeb. Kodeksy takie będą miały charakter wiążący dla przyjmujących je podmiotów, a zatwierdzone przez organ nadzorczy i monitorowane przez podmiot uprawniony wskutek akredytacji GIODO, niewątpliwie pomogą podwyższyć poziom ochrony danych.

To w kodeksie można zawrzeć wskazówki, jak wdrożyć odpowiednie środki bezpieczeństwa oraz wykazać przestrzeganie prawa przez administratora – zwłaszcza jeśli chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko. Co więcej, stosownie do przepisów rozporządzenia, wywiązywanie się z obowiązków tegoż rozporządzenia można wykazać właśnie poprzez stosowanie zatwierdzonego przez GODO kodeksu.

Ułatwieniem dla placówek medycznych może też być kształtowanie architektury określonych rozwiązań technologicznych w oparciu o produkty i usługi, oszacowane uprzednio pod kątem ochrony danych osobowych w czasie procesu certyfikacji. Zastosowanie mechanizmów certyfikacji, znaków jakości i oznaczeń w dziedzinie ochrony danych osobowych będzie wytyczało kierunki rozwoju firm obsługujących sektor ochrony zdrowia ze względu na konieczność zapewnienia przez nie jak najwyższych standardów ochrony danych osobowych. To duże korzyści dla wszystkich.

Problematyka ochrony danych osobowych widziana już oczami nowych unijnych regulacji staje się powoli integralną częścią procesu edukacji na uczelniach medycznych i nie tylko o takim profilu w ramach różnych kierunków studiów. Jest to ważny krok na drodze do zmiany podejścia do tematyki ochrony prywatności przez wszystkich uczestników procesu przetwarzania danych w sektorze zdrowia, a zatem nie tylko lekarzy, pielęgniarki, ratowników medycznych i inne osoby świadczące określone usługi medyczne, ale i cały personel pomocniczy czy wreszcie kadrę zarządzającą.

### **Czy w sektorze ochrony zdrowia nowe technologie to wyzwanie dla ochrony danych?**

Sektor ochrony zdrowia w codziennej działalności chętnie wykorzystuje nowe rozwiązania technologiczne. Służą one przede wszystkim optymalizacji procesu diagnostyki, leczenia czy też profilaktyki zdrowotnej. Przeprowadzanie operacji na odległość, podczas których dane pacjenta często przekazywane są pomiędzy placówkami na terenie Polski, UE i do państw trzecich, wideonadzór na oddziałach intensywnej terapii, zdalny monitoring pacjenta z wszczepionym rozrusznikiem to tylko nieliczne przykłady możliwego wykorzystywania tego typu rozwiązań.

Istotne jest jednak to, aby postępowi technologicznemu towarzyszyły optymalne rozwiązania prawne. Ich brak rodzi stan niepewności i to zarówno po stronie pacjentów/członków ich rodzin, jak i głównie po stronie samych administratorów, co zawsze jest czynnikiem podwyższającym ryzyko właściwej realizacji zadań. Brak na przykład właściwych podstaw prawnych do stosowania telemedycyny, która w praktyce przynosi wiele korzyści pacjentom (oszczędność czasu i środków). Nie ma kompleksowych regulacji dotyczących charakteru konsultacji na odległość, jej zakresu, sposobu przeprowadzenia, zakończenia, dokumentowania (retencji danych), utrwalania na nośnikach czy też usuwania z nich informacji. W tym obszarze mamy raczej do czynienia z praktykami przyjmowanymi przez świadczeniodawców, którzy próbują doregulować to zjawisko w budowanych wewnętrznych procedurach. Opracowywane własne wytyczne - jako że nie są oparte na przepisach prawa - cechuje niejednorodność, a przez to nie są zapewnione tożsame gwarancje dla podmiotów danych, mimo realizacji tych samych celów z wykorzystaniem tych samych danych.

W takich zakresach działalności, co do których nie ma określonych regulacji, na przykład dotyczących biobanków, administrator danych będzie stosował zasady ogólne RODO, co

organ nadzorczy będzie weryfikował w postępowaniach kontrolnych. Podpowiedzią przy wykorzystaniu nowych technologii dla administratora danych będą wskazywane już procesy certyfikacji czy też wykorzystanie postanowień kodeksów postępowania.

Warto zaznaczyć, że obecnie, w związku ze zbliżającym się rozpoczęciem stosowania przepisów ogólnego rozporządzenia o ochronie danych osobowych, konieczne staje się dokonanie przeglądu zarówno przepisów szczególnych regulujących funkcjonowanie placówek medycznych, tak by były zgodne z przepisami rozporządzenia, jak i przeglądu wszelkich przyjętych w danych placówkach rozwiązań czy praktyk, by ustalić, czy dalej mogą być stosowane, czy znajdują one uzasadnienie w przepisach i czy ich wprowadzenie lub też kontynuacja zostały poprzedzone analizą wpływu na prywatność.

Dobłą praktyką powinno stać się podejście oparte na poszanowaniu prywatności osób, których dane dotyczą na jak najwcześniejszym etapie budowania określonych sposobów przetwarzania. Zakłada ono, że ochrona prywatności powinna być brana pod uwagę i stosowana w praktyce przy prowadzeniu wszelkich projektów i działań, tak w sferze publicznej, jak i prywatnej. Ogólne rozporządzenie o ochronie danych czyni tak rozumianą koncepcję privacy by design częścią każdego przedsięwzięcia z udziałem danych osobowych, niezależnie od jego charakteru i celu. Ocena skutków dla ochrony danych staje się natomiast obowiązkiem, jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, co będzie miało miejsce przy przetwarzaniu na dużą skalę szczególnych kategorii danych (np. danych o stanie zdrowia).

Wyzwaniem stojącym przed administratorami danych z sektora ochrony zdrowia będzie także wykazanie, w jaki sposób przy ocenie wprowadzania nowego rozwiązania technologicznego uwzględniona została ochrona danych w fazie projektowania oraz tzw. domyślna ochrona (privacy impact assesment). Taka ocena ma z zasady umożliwić włączanie ochrony prywatności w samo tworzenie projektu, działanie jego składników oraz w zarządzanie technologiami informacyjnymi i systemami przez cały cykl życia informacji. To proaktywne podejście wyrażone przez ww. zasady zakłada, że ochrona prywatności powinna być wbudowana w każdy nowy projekt – co oznacza, że prywatność będzie chroniona nie poprzez dodatki do systemu lub nakładki przygotowane na już istniejące rozwiązania, lecz jest wbudowana w jego konstrukcję tak, że jest po prostu składową projektu. W przypadku systemów teleinformatycznych oznacza to wbudowanie ochrony prywatności zarówno w architekturę systemu, jak i w procesy biznesowe, które system obsługuje – np. poprzez jak najszybszą pseudonimizację danych czy też umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych.

### **Czy rola administratora danych osobowych się zmieni?**

Rozporządzenie zwiększa zarówno samodzielność, jak i odpowiedzialność administratorów danych za przetwarzanie danych osobowych zgodnie z prawem.

Pojęcie administratora na gruncie rozporządzenia nie zmienia się. Administratorem jest ten, kto decyduje o celach i środkach przetwarzania danych. W przypadku sektora medycznego

będzie to zazwyczaj podmiot leczniczy reprezentowany przez dyrektora czy prezesa, bądź osoba prowadząca indywidualną praktykę leczniczą. Jeżeli firma zewnętrzna zostanie wynajęta przez te podmioty do przetwarzania danych, to nie będzie miała statusu administratora danych, ale przetwarzającego dane na zlecenie administratora. Firma zewnętrzna będzie się musiała rozliczyć z wykonywanych zadań, ale nie będzie decydowała o wykorzystywaniu danych. Odpowiedzialność za bezpieczeństwo danych nie będzie mogła być przerzucona wyłącznie na rzecz przetwarzającego na jego zlecenie, choć ten ostatni też musi spełnić odpowiednie warunki, określone w zawartej z nim umowie, np. zapewnić poufność dostępu do danych, przeszkolić pracowników itd.

Bardzo wiele podmiotów nie ma świadomości, że umowa zlecenia związana z przekazaniem obsługi systemu informatycznego na zewnątrz musi się wiązać z zawarciem tzw. umowy powierzenia przetwarzania danych osobowych, a ta będzie musiała zawierać określone elementy. Taki przetwarzający musi zagwarantować, że sam również spełnia zasady ochrony danych osobowych, a rozporządzenie jeszcze dodatkowo wzmacnia pozycję administratora danych osobowych przy zawieraniu takich umów, gdyż wskazuje, że będzie on mógł kontrolować i audytować podmiot, któremu powierzył przetwarzanie swoich danych osobowych. W jaki sposób będzie mógł to zrobić, będzie musiał określić właśnie w umowie powierzenia.

W kontekście zgodnego z prawem przetwarzania danych osobowych warto wspomnieć o jeszcze jednym ważnym ogniwie - administratorze bezpieczeństwa informacji (ABI), który pod rządami RODO będzie nosił miano inspektora ochrony danych. To kluczowa osoba w procesie przygotowania do właściwego stosowania rozporządzenia. To właśnie ABI/inspektor ochrony danych jest w stanie przeprowadzić audyt stanu gotowości danej placówki w tym zakresie. Zarówno pod kątem przyjętych procedur i praktyk, jak i świadomości personelu.

### **Co w zakresie poprawy zachowań pracowników musi zrobić pracodawca?**

Edukacja pracowników w zakresie ochrony danych to niezwykle ważne zagadnienie. To bowiem niski poziom świadomości człowieka prowadzi zazwyczaj do błędów w przetwarzaniu danych osobowych, np. ujawnienia danych osobowych podmiotom nieuprawnionym. Dotyczy to nie tylko personelu medycznego, ale również personelu pomocniczego, czyli wszystkich, którzy mają kontakt z danymi osobowymi pacjentów.

W przypadku personelu pomocniczego to szczególnie ważne, bowiem lekarze czy pielęgniarki oraz inne osoby wykonujące zawody medyczne obowiązują tajemnice zawodowe określone w przepisach sektorowych i ich zachowanie może być poddane weryfikacji w ramach szczególnej odpowiedzialności dyscyplinarnej przed samorządami zawodowymi. Natomiast obowiązki personelu pomocniczego w tym zakresie wynikają jedynie z ogólnych przepisów o ochronie danych osobowych. Dlatego ważne jest, by osoby te były ich świadome. GODO niejednokrotnie podkreśla, że zazwyczaj to człowiek jest najsłabszym ogniwem systemu zabezpieczeń. Wydaje się bowiem, że od strony prawnej mamy dobre rozwiązania dotyczące zabezpieczenia danych przed nieuprawnionym dostępem. Wielokrotne nowelizacje przepisów sektora ochrony zdrowia niewątpliwie uszczelniły proces przetwarzania danych pacjentów. Dlatego istotne jest przestrzeganie przepisów prawa i opracowanych na ich podstawie procedur, by dane osobowe były należycie chronione i dzięki temu bezpieczne.

Niemniej warto wskazać, że pod rządami RODO sytuacja w zakresie zabezpieczania danych osobowych istotnie się zmieni.

W ogólnym rozporządzeniu nie znajdziemy bowiem szczegółowych wskazówek, jakie środki organizacyjne i techniczne należy wdrożyć. Rozporządzenie zachęca jedynie do skorzystania z określonych instrumentów prawnych (zasada minimalizacji, przywoływane zasady privacy, kodeksy postępowania, certyfikacja i in.) oraz narzędzi pseudonimizacji czy też szyfrowania danych. Nie będzie już rozporządzenia wykonawczego do ustawy o ochronie danych osobowych w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych ani przepisów wykonawczych określających szczegółowo sposoby realizacji przez administratora bezpieczeństwa informacji (wkrótce inspektora ochrony danych) kontroli przetwarzania danych u administratora.

Zgodnie z zasadą rozliczalności, to administrator danych – uwzględniając aktualny stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres i cele przetwarzania danych – samodzielnie będzie decydował, jakie środki bezpieczeństwa wdrożyć, by zapewnić zgodność przetwarzania danych z wymogami rozporządzenia. Może więc uznać, że od maja 2018 r. nadal aktualne pozostaną środki techniczne i organizacyjne wdrożone i udokumentowane w dotychczasowej polityce bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym, albo też podjąć decyzję o wdrożeniu zupełnie nowych środków.

Ważne, by oceniając stopień bezpieczeństwa przetwarzanych danych osobowych, uwzględnić przede wszystkim ryzyko wiążące się z przetwarzaniem – wynikające np. z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Zatem to administrator danych będzie decydował, w jaki sposób zapewnić bezpieczeństwo danych - poprzez dobór jakich ludzi, jakich narzędzi programowych czy jakich rozwiązań organizacyjnych. Administrator będzie musiał brać pod uwagę z jednej strony głosy klientów komunikujących swoje wątpliwości w procesie zarządzania ich danymi, a z drugiej głosy pracowników, którzy informują, gdzie są problemy, gdzie występują stany niepewne, gdzie pojawiają się nowe zagrożenia i nowe wyzwania. Wielką rolę w procesie analizy wszystkich sygnałów będzie pełnił inspektor ochrony danych.

### **Nie będzie już potrzebna rejestracja zbioru danych osobowych. Co ją zastąpi?**

Procesy dotyczące przetwarzania danych będą musiały być ujęte w rejestry przetwarzania; nie będzie bowiem rejestracji zbiorów danych osobowych w GODO. Poza tym będą prowadzone rejestry naruszeń, które to naruszenia w określonych sytuacjach będą musiały być zgłaszane do GODO, a niekiedy również komunikowane pacjentowi. Rozporządzenie zakłada także pewne sytuacje, kiedy takie informowanie nie będzie konieczne, ale będą to wyjątki, zasada będzie informowanie.

Placówki, które nie wdrożyły u siebie odpowiednich procedur, odpowiednich zasad, nie mają opracowanej odpowiedniej dokumentacji czy przygotowanego systemu informatycznego spełniającego wymogi prawne będą musiały poczynić pewne dodatkowe inwestycje, co wiąże



się z kosztami. Pamiętać jednak należy, iż takie koszty należało zakładać od początku rozpoczęcia procesu przetwarzania danych, a ten jest zwykle realizowany w placówkach od wielu lat. Dodatkowo długi czas obowiązywania przepisów o ochronie danych osobowych w Polsce pozwolił odpowiedzialnym administratorom danych sukcesywnie wprowadzać konieczne zmiany związane z ochroną danych.

Bardzo wiele placówek opieki zdrowotnej musi przyrzeć się dotychczasowym procedurom i rozwiązaniom. Szczególną troskę powinny wykazać osoby prowadzące indywidualne praktyki lekarskie, gdyż w ich przypadku poziom przygotowania do stosowania zasad określonych w rozporządzeniu jest bardzo niski. Dotąd bowiem te podmioty, jako mali przedsiębiorcy, nie zakładały konieczności wprowadzania zasad ochrony danych, a temat ten, w świetle napływających komunikatów o wysokościach grożących kar, zaczyna dopiero być przez nie analizowany.

Tymczasem poziom zagrożeń związanych z nieuprawnionym dostępem do danych medycznych sukcesywnie wzrasta. Jak bardzo ważna jest zmiana podejścia w tym zakresie, niech świadczy chociażby fakt, że w II kwartale 2017 roku 27 procent incydentów związanych z atakami na systemy informatyczne stanowiły incydenty dotyczące sektora ochrony zdrowia.

Standardem wielu placówek jest przesyłanie informacji w postaci niezaszyfrowanej, co jest już krokiem do ich przejęcia przez podmioty nieuprawnione. Musimy pamiętać, iż dane o stanie zdrowia czy dane genetyczne, stają się coraz bardziej poszukiwanym, a przez to coraz bardziej cennym towarem.

### **Co grozi placówkom, które dopuszczają do wycieku danych osobowych pacjentów?**

Pod rządami RODO odpowiedzialność administratorów za wyciek będzie bardziej dolegliwa, a osoby, których dane dotyczą, zyskają nowe narzędzia dochodzenia swoich praw. Gdy placówki nie zastosują odpowiednich procedur i dane pacjentów wyciekną, będą oni mogli – co jest nowością - złożyć wniosek o odszkodowanie za naruszenie prawa do ochrony danych osobowych, zyskując bezpośrednio prawo do wyegzekwowania tego odszkodowania przed sądem.

Pacjenci będą też mogli złożyć skargę do Generalnego Inspektora Ochrony Danych Osobowych, który będzie miał możliwość nałożenia dotkliwych administracyjnych kar pieniężnych.

Dzisiaj pacjenci gdy uznają, że poprzez wyciek danych doszło do naruszenia ich dóbr osobistych, mogą wystąpić do sądu cywilnego o odszkodowanie. Musieliby jednak wiedzieć, że do takiego incydentu doszło, a najczęściej administratorzy nie informują ich o tym fakcie. Rozporządzenie stanowi zaś, że administrator będzie miał obowiązek poinformować o takich zdarzeniach.

Administratorzy danych będą zaś musieli prowadzić rejestr naruszeń, odnotowywać, na czym polegało naruszenie i jakie kroki podjęto w związku z zaistnieniem określonego incydentu.

Ci administratorzy, u których nawet dojdzie do naruszeń ochrony danych, ale zgłoszą ten fakt do GIODO i poinformują o podjętych środkach, aby zapobiec takim zdarzeniom w przyszłości, będą w lepszej sytuacji niż ci, którzy będą to ukrywać. Nieujawnianie informacji o naruszeniach będzie się wiązać z odpowiedzialnością administracyjną i karną.

### **Jak GIODO będzie wspierał administratorów danych?**

Nowe przepisy dają GIODO możliwość wspierania administratorów danych. Administrator, który po dokonaniu oceny ryzyka uzna, że potwierdza ona wysokie ryzyko dla ochrony danych osobowych i niezbędne jest zastosowanie środków minimalizujących zagrożenie, będzie mógł zwrócić się do GIODO o wsparcie w ramach tzw. konsultacji. Rozporządzenie zapewnia współpracę pomiędzy inspektorem danych osobowych a organem nadzorczym.

Warto jednak zaznaczyć, że choć rozporządzenie wprowadza nowe mechanizmy ochrony danych osobowych, to jednak większość dotychczasowych zasad nie traci swej aktualności. Dlatego wiele rozstrzygnięć GIODO czy orzeczeń sądów zachowuje aktualność. Zatem ci administratorzy, którzy dotąd rzetelnie realizowali swoje obowiązki, śledzili decyzje i opinie GIODO, uczyli się na błędach swoich kolegów, łatwiej dostosują swoją działalność do przepisów rozporządzenia i łatwiej im będzie wytłumaczyć pracownikom, jak ważne jest uwzględnianie przepisów o ochronie danych osobowych na każdym poziomie ich aktywności zawodowej.

### **Czy regulacje krajowe zostały dostosowane do RODO?**

Rozporządzenie to podstawowy akt prawny regulujący zasady przetwarzania danych osobowych. Przepisy krajowe powinny jedynie doprecyzować postanowienia RODO oraz dostosować krajowy porządek prawny do zawartych w nim regulacji i zasad. Dlatego tak ważne jest, by zostały stworzone z najwyższą starannością i nie prowadziły do obniżenia standardów ochrony danych ustanowionych w RODO.

Jest to tym bardziej istotne, że wiele podmiotów jest zainteresowanych zyskaniem dostępu do informacji dotyczących pacjentów – by wymienić tylko pracodawców, firmy ubezpieczeniowe czy banki. Dlatego ustawodawstwo krajowe w tym zakresie powinno być stworzone tak, by minimalizować wykorzystywanie danych medycznych w innych celach niż te, które są związane z leczeniem pacjenta. Dane o stanie zdrowia są bowiem „wyśmienitym” towarem na rynku, cieszą się dużym zainteresowaniem i będą się cieszyć jeszcze większym, z uwagi na swoją unikalność i swój zakres.

W mojej ocenie w Polsce nie wszystkie regulacje dostosowane są do przepisów RODO, choć istniejący stan prawny jest zdecydowanie lepszy niż ten, z jakim GIODO miał do czynienia jeszcze kilka lat temu. Świadomość wzrasta sukcesywnie także po stronie projektodawców. Istnieją jednakowoż takie luki prawne, które powinny być jak najszybciej wyeliminowane. Przykładem może być biobankowanie. Mamy wprawdzie ustawę o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów, ale w praktyce nie obejmuje ona działalności biobanków, które gromadzą materiał do celów naukowych, albo komercyjnych gdyż wspomniany akt prawny reguluje jedynie działalność biobanków związaną z celami klinicznymi. Brak organu, który miałby nadzorować działalność biobanków działających w ww. celach powoduje, że mamy na rynku podmioty prowadzące działalność gospodarczą, które za zgodą pacjentów takie dane przechowują i nie ma żadnych regulacji dotyczących tego, co dalej z tymi informacjami może się dzieć.

Kontrole przeprowadzone kilka lat temu wykazały, że niektóre firmy prowadzące biobanki w ogóle nie mają świadomości, że przetwarzają dane osobowe. Jednak dane genetyczne, nawet pseudonimowe, w określonych okolicznościach muszą być traktowane jako dane osobowe. Co do tego nie ma wątpliwości zarówno na gruncie ustawy o ochronie danych osobowych, jak i przepisów rozporządzenia.

Generalny Inspektor Ochrony Danych Osobowych przygląda się uważnie pracom związanym z regulacjami dedykowanymi tematyce ochrony danych wrażliwych. Dokonywana jest taka analiza zarówno w procesie konsultacji wpływających do organu projektów aktów prawnych, jak i poprzez udział w charakterze konsultanta w pracach wielu zespołów, np. zespołu, który powstał przy ministrze nauki i szkolnictwa wyższego, a który wypracowuje pewne wytyczne do wprowadzenia regulacji poświęconych biobankowaniu. Znajdujemy się w momencie, w którym mamy jeszcze szansę wprowadzić lepsze rozwiązania prawne od istniejących, a także uregulować materie pozostające do tej pory poza marginesem zainteresowania ustawodawcy. Niewątpliwie GODO będzie wspierał wszelkie inicjatywy, które będą dążyć do osiągnięcia ww. celów, ale - co wymaga podkreślenia - nie może projektodawcy zastępować w przygotowywaniu określonych rozwiązań.

Rozmawiała: Magdalena Okoniewska