RODO w ochronie zdrowia - przewodnik po zmianach w zakresie ochrony danych osobowych

Autor:Łokaj Maciej **Rodzaj:** komentarz praktyczny

1. Kiedy wchodzą w życie nowe regulacje?

W dniu 25 maja 2016 roku weszło w życie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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), nazywane dalej RODO. Już na wstępie należy wyjaśnić czytelnikom, iż w przypadku RODO **konieczne jest wyraźne rozróżnienie daty wejścia w życie rozporządzenia, tj. 25 maja 2016 roku, od daty rozpoczęcia jego stosowania, tj. 25 maja 2018 roku**. Powyższe wywołuje bowiem niejednokrotnie pewne zamieszanie.

2. Krajowe przepisy doprecyzują RODO

Jak wynika z treści preambuły do rozporządzenia, niniejszy unijny akt prawny przyjęty został przede wszystkim w związku z szybkim postępem technicznym i postępującą globalizacją, a co się z tym wiąże, zagrożeniami związanymi z przepływem danych osobowych osób fizycznych, głównie związanymi z działaniem w Internecie (pkt 6 i 9 preambuły). Nadto, unijny prawodawca zwrócił uwagę na występujące różnice w stopniu ochrony danych osobowych obywateli w państwach członkowskich UE. Stąd też, kolejnym celem RODO jest zrównoważenie przedmiotowej ochrony w całej Unii. Już w tym miejscu jednak należy podkreślić, iż rozporządzenie **pozostawia państwom członkowskim możliwość doprecyzowania jego przepisów, zwłaszcza w odniesieniu do przetwarzania danych osobowych szczególnych kategorii**, a zatem tzw. wrażliwych danych osobowych, do której zaliczają się również dane dotyczące zdrowia osób fizycznych (pkt 10 preambuły).

3. Co jest daną osobową w ochronie zdrowia?

Należy podkreślić, iż RODO już na etapie preambuły definiuje pojęcie danych osobowych dotyczących zdrowia. Zgodnie bowiem z pkt 35 preambuły za takie dane uważane są wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia konkretnej osoby. Unijny ustawodawca zalicza do danych medycznych także informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym, co jest nowością w szczególności punktu widzenia obowiązujących do tej pory krajowych przepisów, **dane genetyczne i próbki biologiczne** oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro. W tym miejscu, należy zwrócić uwagę czytelników na kolejną nowość dotyczącą zakresu danych medycznych, albowiem zgodnie z treścią pkt 35 preambuły RODO do danych dotyczących zdrowia zaliczają się **także numery, symbole lub oznaczenia przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych**, przy czym, co kluczowe, chodzi tutaj o oznaczenia nadawane nie tylko podczas świadczenia usług opieki zdrowotnej, ale także rejestracji do tych usług. Tym samym unijny prawodawca wprowadził jednoznaczną zasadę, iż **już na etapie rejestracji pacjenta na przykład w poradni jego dane osobowe, które są związane z udzielaniem świadczeń opieki zdrowotnej, zaliczane są do kategorii danych wrażliwych, podlegających szczególnej ochronie.** Pomimo, iż rozporządzenie unijne utrzymuje zasadę generalnego zakazu przetwarzania wrażliwych danych osobowych osób fizycznych, w tym danych medycznych, dopuszcza ono wyjątki od tej zasady, ze względu na cele zdrowotne, w tym związane ze zdrowiem publicznym oraz zarządzaniem usługami opieki zdrowotnej (pkt 52 preambuły). Unijny ustawodawca kładzie szczególny nacisk na możliwość przetwarzania danych osobowych osób fizycznych, w tym danych medycznych, ze względu na interes publiczny w dziedzinie zdrowia publicznego, dopuszczając, co szczególnie ważne, możliwość przetwarzania takich danych bez konieczności uzyskiwania zgody osoby, której dane dotyczą, co stanowi odzwierciedlenie dotychczas obowiązujących krajowych przepisów prawa w tym zakresie, zezwalających placówkom ochrony zdrowia na przetwarzanie danych medycznych pacjentów, z mocy prawa, bez wymogu pozyskiwania ich zgody.

Artykuł 4 RODO definiuje dane osobowe jako **informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej** tj. osobie, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Rozporządzenie, w sposób jednoznaczny definiuje również, pojęcie danych dotyczących zdrowia, czyli danych osobowych o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia.

4. Kto jest odpowiedzialny za przetwarzanie danych osobowych w placówce medycznej?

Jak już wskazano wcześniej, RODO utrzymuje podział danych osobowych, na te które można określić jako **podstawowe**, umożliwiające identyfikację oraz tzw. dane szczególne, czyli **sensytywne** dane osobowe, do których zaliczone zostały także dane dotyczące zdrowia osoby fizycznej. Rozporządzenie wprowadza również w art. 10 generalny zakaz przetwarzania danych wrażliwych, przy zachowaniu szeregu wyjątków. W zakresie danych obejmujących informacje o stanie zdrowia danej osoby, ich przetwarzanie dopuszczalne jest pod warunkiem, że jest to niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego lub jest to niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych. Warto w tym miejscu zwrócić uwagę czytelników, iż unijny prawodawca

wprowadza w treści rozporządzenia niezwykle ważny zapis dotyczący podmiotu odpowiedzialnego za przetwarzanie danych medycznych w związku z udzielaniem świadczeń opieki zdrowotnej.

Zgodnie z art. 10 ust. 3 RODO, odpowiedzialność za przetwarzanie medycznych danych osobowych ponosi pracownik podlegający obowiązkowi zachowania tajemnicy zawodowej, co zdaniem autora, w praktyce oznacza, że np. w przypadku, kiedy dane medyczne przetwarzać będzie sekretarka medyczna na polecenie ordynatora lub kierownika oddziału i w związku z tym przetwarzaniem dojdzie do naruszenia obowiązujących przepisów, odpowiedzialność z tego tytułu poniesie bezpośrednio zlecający konkretne zadanie ordynator lub kierownik, będący lekarzem, czyli osobą zobowiązaną do zachowania tajemnicy zawodowej.

Na koniec tej części rozważań należy zauważyć, iż poprzez stosowne zapisy art. 10 ust. 4 RODO, unijny prawodawca pozostawia państwom członkowskim UE swobodę w zakresie możliwości wprowadzenia dodatkowych warunków, również ograniczających, w odniesieniu do przetwarzania danych dotyczących zdrowia.

5. Obowiązki placówki medycznej jako administratora danych

Informacyjne

Wśród obowiązków podmiotu wykonującego świadczenia zdrowotne, rozporządzenie wyróżnia, w pierwszej kolejności **obowiązki, które należy zaliczyć do grupy informacyjnych**. Placówka medyczna zobowiązana jest do udzielania osobie, której dane osobowe zostały pozyskane, informacji dotyczących między innymi swoich danych kontaktowych, danych inspektora danych osobowych (która to funkcja będzie obligatoryjna w jednostkach ochrony zdrowia, o czym dalej), celu przetwarzania oraz odbiorcach danych osobowych i kategoriach tychże odbiorców (art. 13 i 14 RODO). Informacje te winny być przekazywane w przejrzystej zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem (art. 12 RODO). Nadto osobie, której dane medyczne są przetwarzane, przysługuje prawo dostępu do swoich danych, a także prawo do ich sprostowania (art. 15 i 16 RODO). Jednocześnie placówka medyczna będąca administratorem danych ma obowiązek zareagować na każde żądanie dostępu czy sprostowania i poinformować żądającego o podjętych działaniach nie dalej niż w ciągu miesiąca od otrzymania żądania, a w przypadkach szczególnie skomplikowanych nie dłużej niż w ciągu łączenie trzech miesięcy (art. 12 RODO).

Techniczne i organizacyjne

Administrator danych ma również obowiązek wdrożyć wszelkie niezbędne środki techniczne i organizacyjne w celu zapewnienia przetwarzania danych w sposób zgodny z unijnym rozporządzeniem. Należy w tym miejscu zwrócić uwagę na brzmienie art. 24 ust. 2 RODO, zgodnie z którym jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki o których mowa wyżej winny obejmować wdrożenie przez administratora odpowiednich polityk ochrony danych. Wydaje się, iż w powyższym zakresie konieczna będzie, w szczególności, weryfikacja treści stosowanych obecnie przez placówki medyczne polityk bezpieczeństwa danych osobowych, czyli dokumentów powstałych w oparciu o treść rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych i ich dostosowanie do wymogów unijnego rozporządzenia.

6. Powierzenie przetwarzania - czy zawsze konieczna jest umowa?

Spore zmiany czekają placówki medyczne, które dysponują umowami powierzenia przetwarzania danych osobowych. Unijne rozporządzenie, w treści art. 28, w sposób wyraźny i jednoznaczny wprowadza obowiązek zawierania pisemnych umów powierzenia przetwarzania. Co ciekawe, unijny prawodawca dopuszcza również jako formę pisemną umowy formę elektroniczną. Zgodnie z przepisem wskazanym powyżej, umowa winna stanowić w szczególności, że podmiot, któremu powierzone zostało przetwarzanie danych:

1) dokonuje tego wyłącznie na udokumentowane polecenie administratora,

2) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

3) podejmuje wszelkie niezbędne środki bezpieczeństwa dla ochrony przetwarzanych danych,

4) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o ile dysponuje szczegółową i pisemną zgodą administratora danych na dalsze powierzenie,

5) w miarę możliwości wspiera administratora w zakresie wywiązywania się przez niego z obowiązków związanych z ochroną danych osobowych, nałożonych treścią rozporządzenia, a także udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia powyższych obowiązków,

6) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo nakazują przechowywanie danych osobowych,

7) umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji,

7. Rejestr czynności przetwarzania

Szczegółowa analiza unijnego rozporządzenia prowadzi do wniosku, że **zniesiony zostaje obowiązek rejestracji zbiorów danych osobowych** w mającym docelowo powstać na miejsce GIODO, Urzędzie Ochrony Danych Osobowych. Powyższe niewątpliwie wyeliminuje wątpliwości dotyczące określonych zbiorów danych, którymi dysponują placówki medyczne, a związane z faktem podlegania lub nie podlegania ustawowemu zwolnieniu z obowiązku rejestracji. Nie mniej, jak wynika z treści art. 30 RODO, podmioty i instytucje przetwarzające dane wrażliwie, a zatem również dane medyczne, zobowiązane będą do **prowadzenia rejestru czynności przetwarzania danych osobowych, który zawierać będzie, w szczególności:**

1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także inspektora ochrony danych,

2) cele przetwarzania,

3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,

4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,

5) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,

6) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,

Rejestr będą również zobowiązane prowadzić podmioty, którym placówki medyczne powierzyły przetwarzanie danych medycznych. Rozporządzenie sankcjonuje obowiązek prowadzenia rejestrów w formie pisemnej, w tym także w formie elektronicznej.

8. Ocena skutków dla ochrony danych - nowy obowiązek

Ze względu na fakt przetwarzania sensytywnych danych osobowych, placówki medyczne będą również zobowiązane do **dokonania oceny skutków dla ochrony danych**. W oparciu o art. 35 RODO, dokument oceny będzie zawierać ma co najmniej:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania,

2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,

3) ocenę ryzyka naruszenia praw lub wolności osób fizycznych (pacjentów), których dane dotyczą,

4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie unijnego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy,

9. IOD zamiast ABI

Z dniem rozpoczęcia stosowania unijnego rozporządzenia, czyli 25 maja 2018 roku, placówki ochrony zdrowia zobowiązane będą do posiadania Inspektora Ochrony Danych (IOD), która to funkcja zastąpi obecnego Administratora Bezpieczeństwa Informacji (ABI).

Jest to dość zasadnicza zmiana, albowiem do tej pory posiadanie ABI miało charakter fakultatywny, tymczasem od wskazanej wyżej daty, wyznaczenie Inspektora w jednostkach medycznych będzie obligatoryjne.

Zgodnie z art. 37 RODO, Inspektor może wykonywać swoje zadania na podstawie umowy o pracę jak i umowy cywilnoprawnej. Podstawą wyznaczenia Inspektora są jego kwalifikacje zawodowe, a w szczególności wiedza fachowa z zakresu prawa i praktyk w dziedzinie ochrony danych osobowych. W oparciu o art. 39 RODO, Inspektor ma następujące główne zadania:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów i doradzanie im w tej sprawie,

2) monitorowanie przestrzegania niniejszego rozporządzenia oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,

3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,

4) współpraca z organem nadzorczym, tj. Urzędem Ochrony Danych Osobowych,

10. Zgłaszanie naruszenia danych osobowych, czyli tzw. autodonos

Kolejną istotną nowość z punktu widzenia placówek medycznych stanowić będzie, wynikający z art. 33 RODO, **bezwzględny obowiązek informowania Urzędu Ochrony Danych Osobowych o każdym stwierdzonym naruszeniu zasad ochrony danych osobowych**. Niespełnienie powyższego obowiązku wiązać się może z nałożeniem wysokich administracyjnych kar pieniężnych, o czym niżej. Zgłoszenie nie jest konieczne w przypadku jeżeli jest mało prawdopodobne, by skutkowało ono naruszenie praw lub wolności osób fizycznych. **Zgłoszenie naruszenia winno nastąpić najdalej w ciągu 72 godzin od jego stwierdzenia** i musi co najmniej:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych, od którego można uzyskać więcej informacji,

3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków,

Nadto, zgodnie z art. 34 RODO, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamiać ma także osobę, której dane dotyczą, o takim naruszeniu. Naruszenie także tego obowiązku również wiązać się może z nałożeniem wysokich kar pieniężnych.

11. Kary pieniężne

Na koniec należy wskazać, iż znaczącą nowość, zestawiając chociażby z dotychczas obowiązującą w Polsce ustawą o ochronie danych osobowych, stanowi wysokość kar pieniężnych o charakterze administracyjnym, jakie mogą być nakładane na podmioty naruszające regulacje zawarte w rozporządzeniu unijnym dotyczące ochrony danych osobowych. Autor zwraca uwagę czytelników na fakt, iż stwierdzenie określonych naruszeń omawianego rozporządzenia może skutkować w stosunku do placówki medycznej karą pieniężną w maksymalnej wysokości do 20.000.000 euro, w przypadku publicznych jednostek ochrony zdrowia i do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w odniesieniu do placówek medycznych będących przedsiębiorcami.

RODO nie wskazuje środków i metod zabezpieczania danych, jedynie daje wskazówki

Placówki medyczne na terenie całej Unii Europejskiej od 25.05.2018 roku będą zobowiązane do stosowania nowego unijnego rozporządzenia dotyczącego ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnego przepływu takich danych (RODO). Zmienia ono perspektywę i podejście do ochrony danych osobowych, w tym do ich zabezpieczania – mówi dr inż. Andrzej Kaczmarek, dyrektor Departamentu Informatyki w Biurze Generalnego Inspektora Ochrony Danych Osobowych.

Co zmieni RODO w zakresie bezpieczeństwa danych osobowych?

Podstawowa zmiana wiąże się z tym, że RODO nie wskazuje środków technicznych i organizacyjnych, jakie administrator danych powinien zastosować w celu zapewnienia właściwej ochrony przetwarzanym danym. Dotyczy to zarówno danych przetwarzanych w sposób tradycyjny (spisy, kartoteki, skorowidze, wykazy, a także wszelkie pisma występujące w postaci papierowej), jak i danych przetwarzanych przy użyciu systemów informatycznych. RODO stanowi jedynie, że środki, jakie administrator zobowiązany jest zastosować, powinny być odpowiednie do zakresu, kontekstu i celu, a także ryzyka naruszenia ochrony przetwarzanych danych. W tym akcie prawnym nie znajdziemy jednak podpowiedzi, jakie środki bezpieczeństwa należy zastosować w celu minimalizacji ryzyka, jak ocenić ryzyko, ani żadnej metodyki w tym zakresie. Nie znajdziemy również wyjaśnienia, co tak naprawdę oznacza to, że środki jakie zastosujemy, mają być odpowiednie i jaką przyjąć miarę dla ich oceny. RODO stanowi jedynie, że przy ocenie ryzyka i ustanawianiu zabezpieczeń minimalizujących to ryzyko należy uwzględnić stan wiedzy technicznej, koszt wdrażania, a także skutki, jakie urzeczywistnienie się zidentyfikowanych zagrożeń może powodować dla osób, których dane są przetwarzane. Art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2017 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 (RODO) przesądza zaś, że na potrzeby zapewnienia właściwego bezpieczeństwa, wdrożyć należy odpowiednie środki techniczne i organizacyjne, w tym takie jak:

- pseudonimizacja i szyfrowanie danych osobowych,

- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Dlatego teraz musimy nauczyć się nowego podejścia, zgodnie z którym, podejmując decyzje o zastosowaniu określonych środków bezpieczeństwa, należy uwzględnić wartość, jaką mają przetwarzane dane, kontekst, w jakim są one przetwarzane oraz skutki, jakie może wywołać ich naruszenie tj. ich nieuprawnione ujawnienie, modyfikacja, zbyt długa niedostępność lub utrata. Przykładem może być zagrożenie utraty ciągłość dostępu do danych. W przypadku sklepu internetowego, ciągłość jest bardzo istotna, zwłaszcza dla właściciela sklepu, bo przekłada się na straty związane ze zmniejszeniem obrotów (klient może zamówić towar w innym sklepie), ale nie krytyczna (klient może zamówić towar później). Natomiast w przypadku usług medycznych brak ciągłości działania, np. w zakresie dostępu do danych medycznych lub usług, może powodować konsekwencje w postaci utraty zdrowia, a nawet życia.

Uwzględnienie kontekstu przetwarzania danych to niezbędny element podejścia opartego na ryzyku. Tylko pełne informacje o kontekście użycia danej informacji pozwolą na rzetelną ocenę skutków związanych z jej brakiem, przekłamaniem lub nieuprawnionym ujawnieniem. Kontekst to również czynniki, które mogą spowodować utratę, nieuprawnione wykorzystanie lub brak dostępu do przetwarzanych danych.

Zatem zasadniczą zmianą, jaką RODO wprowadza w zakresie bezpieczeństwa danych, jest właśnie takie ogólne spojrzenie na środowisko, w jakim dane są przetwarzane oraz na związane z nim zagrożenia utraty, niewłaściwego lub nieuprawnionego użycia, a także na skutki, jakie może to powodować głównie dla osób, których dane dotyczą.

Efektem przyjęcia takiego podejścia będzie to, że stosowane zabezpieczenia w bardzo dużym stopniu zależne będą od wielkości i złożoności środowiska, w którym dane są przetwarzane, ilości źródeł, z których dane są pozyskiwane czy liczby punktów, do których są przekazywane. Ważny będzie też kontekst i rodzaj przetwarzanych danych, a zwłaszcza ich wrażliwość, jak np. w przypadku danych dotyczących stanu zdrowia, kodu genetycznego, preferencji seksualnych, politycznych itp.

Inne będą również wymagania dotyczące poziomu zabezpieczenia danych przetwarzanych w gabinecie lekarza prowadzącego indywidualnie praktykę lekarską, a inne w gabinecie lekarza w szpitalu. W tym pierwszym przypadku w gabinecie znajduje się najczęściej tylko jeden komputer, na którym pracuje wyłącznie właściciel gabinetu, wykorzystując go do prowadzenia dokumentacji medycznej, wystawiania recept i prowadzenia rozliczeń z NFZ. W przypadku szpitala komputer w gabinecie lekarza połączony będzie najczęściej z centralnym systemem rejestracji pacjentów w tej placówce i wykorzystywany nie przez jednego,

lecz wielu lekarzy. Ponadto komputer ten może być połączony z wieloma innymi wzajemnie połączonymi urządzeniami. W tym ostatnim przypadku wiele urządzeń może posiadać tak zwane adresy publiczne, widoczne z zewnątrz, co sprawia, że przetwarzane przy jego użyciu dane są bardziej narażone na ataki cyberprzestępców, którzy mogą zainfekować komputer w celu wyłudzenia okupu czy wykradzenia danych. I to nie są nierealne opowieści, bo nie tylko na świecie, ale również Polsce takie sytuacje się zdarzają. W niektórych przypadkach nawet wpłacenie żądanego okupu nie powoduje odblokowania dostępu do danych.

Co powinny zrobić placówki medyczne przygotowując się na RODO?

Placówki, które stosowały zabezpieczenia danych zgodnie z wymaganiami obecnie obowiązujących przepisów, nie będą miały wiele pracy. Obecne regulacje prawne wymagały bowiem, aby przetwarzane dane zabezpieczone były przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem odpowiednio do zagrożeń oraz kategorii danych objętych ochroną. Żeby takie „odpowiednie do zagrożeń oraz kategorii danych" zabezpieczenia zastosować, administrator musiał przede wszystkim zidentyfikować występujące zagrożenia dla ochrony danych i ocenić ich istotność oraz prawdopodobieństwo wystąpienia.

Podmioty, które taką analizę przeprowadziły, powinny jedynie zweryfikować, czy w międzyczasie w strukturze przetwarzania lub stosowanych zabezpieczeniach nie dokonywano takich zmian lub uzupełnień, które mogły mieć wpływ na bezpieczeństwo danych. Jeśli takie zmiany były, powinny ponownie dokonać analizy ryzyka oraz przeprowadzić analizę skutków dla ochrony danych, o której mowa w art. 35 RODO. Należy przy tym zaznaczyć, że dla podmiotów, które przeprowadziły analizę ryzyka i mają ten proces udokumentowany, przeprowadzenie oceny skutków dla ochrony danych nie powinno być wielkim problemem. Do analizy skutków dla ochrony danych mogą one zastosować metodykę, którą stosowały do oceny ryzyka, zmieniając jedynie kryteria identyfikacji zagrożeń i oceny skutków, ukierunkowując je na te elementy, które mogą naruszać prawa i wolności osób, których dane dotyczą. Nie należy oczywiście zapominać przy tym o dodatkowych wymaganiach prawnych, jakie nałożone są przez prawo krajowe, w tym na dodatkowe warunki i wymagania dotyczące przetwarzania dokumentacji medycznej wskazane m. in. w ustawie z 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, ustawie z 28.04.2011 r. o systemie informacji w ochronie zdrowia oraz rozporządzeniu Ministra Zdrowia z 9.11.2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

Jak należy zabezpieczać dane medyczne?

Do informacji medycznych dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób powinny mieć dostęp tylko osoby uprawnione. W związku z tym powinna być przeprowadzona odpowiednia klasyfikacja przetwarzanych informacji i określenie, kto jest uprawniony do ich przetwarzania i w jakim zakresie. Do innego zakresu informacji powinien mieć dostęp lekarz biorący udział w leczeniu danego pacjenta, do innego zakresu pielęgniarka czy osoba pracująca w recepcji placówki medycznej. Uprawnienia te powinny być przydzielone zależnie od sprawowanej funkcji i wykonywanego zakresu obowiązków. Zalecane są takie systemy, gdzie uprawnienia dostępu do danych uzależniane są w pewnym stopniu od miejsca, jakie użytkownik zajmuje w strukturze organizacyjnej danej instytucji (szpital, przychodnia, laboratorium) i przydzielane są z uwzględnieniem wykonywanych zadań (ról).

Na przykład dla osoby zatrudnionej na stanowisku pielęgniarki na oddziale X, domyślnie powinny być przypisywane uprawnienia dostępu do danych osób leczonych tylko na tym oddziale. W przypadku, gdy wystąpi potrzeba obsługi pacjentów innego oddziału, uprawnienia te powinny być stosownie zmodyfikowane. Ich zakres z kolei powinien być odpowiedni do czynności, które ta pielęgniarka wykonuje lub ma prawo wykonywać, w zakresie przydzielonych jej zdań.

Uprawnienia takie dodatkowo mogą być profilowane w zależności od stażu pracy, wykształcenia i kategorii stanowiska. Dla osoby zatrudnionej w izbie przyjęć, której zadaniem jest obsłużenie każdego zgłoszenia, uprawnienia będą dotyczyć w odpowiednim zakresie przetwarzania danych wszystkich osób, niezależnie od wydziału czy oddziału, do jakiego będą skierowane.

Przy nadawaniu uprawnień należy pamiętać o zasadzie celowości i zasadzie minimalizacji, co oznacza, że zakres nadawanych uprawnień powinien być zgodny z celem przetwarzania danych i jednocześnie minimalny, aby cel ten osiągnąć.

Placówki nie zawsze się do tego stosują. Często przydzielany jest dostęp do pełnego zakresu informacji, niezależnie od tego, czy osoba, której on dotyczy, rzeczywiście go potrzebuje do wykonywania swoich zadań. Takie rozwiązanie nie jest właściwe, gdyż stanowi zaprzeczenie zasady minimalizacji i adekwatności, o których jest mowa w art. 5 RODO.

System informatyczny do przetwarzania danych osobowych w szpitalu powinien być odpowiednio dopasowany do wielkości organizacji i skonfigurowany odpowiednio do jej struktury organizacyjnej. Podobnie jak systemy obiegu dokumentów. Gdy mamy kilka departamentów lub oddziałów, to jeżeli dokument trafia do sekretariatu głównego, to najpierw otrzymuje go sekretarka, potem sekretariat odpowiedniego departamentu czy oddziału, a na końcu osoba, która zostanie wskazana do załatwienia danej sprawy lub przygotowania i wysłania odpowiedzi. Ważne przy tym jest, aby dostęp do tego dokumentu był ograniczony tylko do pracowników odpowiedniego oddziału lub nawet tylko określonego pracownika i dyrektora. Inaczej może być w przypadku rzecznika prasowego, który powinien wiedzieć, co się dzieje w całej organizacji i mieć dostęp do informacji z różnych oddziałów.

Zatem odpowiadając na pytanie, „Jak należy zabezpieczyć dane medyczne?", odnieść należy się z jednej strony do ogólnej miary skuteczności zabezpieczeń, dla której nie jest istotne, jakiego rodzaju dane podlegają ochronie, z drugiej zaś strony do stopnia szczegółowości tej ochrony i wymagań prawnych, gdzie rodzaj przetwarzanych danych ma istotne znaczenie.

W zakresie skuteczności zabezpieczeń, ze względu na to, że dane medyczne, zgodnie z art. 9 RODO, należą do tzw. szczególnej kategorii danych osobowych, zastosowany poziom bezpieczeństwa powinien być bardzo wysoki. Zatem środki ochrony powinny być odpowiednio niezawodne w działaniu i odporne na wszelkie próby „przełamania" zastosowanych zabezpieczeń. W tym kontekście nie ma znaczenia treść przetwarzanych danych, lecz wyłącznie wymagania dotyczące bezpieczeństwa. W art. 32 RODO podkreśla się, że bezpieczeństwo danych wymaga od systemów informatycznych między innymi właściwości polegających na:

- zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

- zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

Ponadto podkreśla się, że zapewnienie wysokiej skuteczności zastosowanych środków bezpieczeństwa wymaga regularnego ich testowania, mierzenia i oceny. W praktyce zapewnienie wspomnianego wysokiego poziomu ochrony - poza odpowiednimi rozwiązaniami organizacyjnymi - wymaga zastosowania wysokiej klasy urządzeń używanych do przetwarzania danych (serwery, nośniki danych, systemy bezpieczeństwa), które posiadają specjalne rozwiązania konstrukcyjne dublujące działanie niektórych podzespołów, których wymiana jest możliwa w czasie ich pracy w celu zapewnienia wysokiej dostępności realizowanych usług.

W odniesieniu do zakresu i szczegółowości ochrony przetwarzanych danych, w przeciwieństwie do samej jakości zabezpieczeń, istotne są rodzaj i charakter przetwarzanych danych. Szpitale, ośrodki zdrowia i inne placówki medyczne, które przetwarzają dane osobowe swoich pacjentów odnoszące się do stanu ich zdrowia, w zakresie stosowanych zabezpieczeń powinni uwzględniać bardziej szczegółowe wymagania dotyczące bezpieczeństwa. Wymagania te powinny przede wszystkim uwzględniać elementy związane z kontrolą dostępu do danych, które szczegółowo uregulowane zostały w przepisach prawa odnoszących się do przetwarzania dokumentacji medycznej. W odniesieniu do dokumentacji medycznej jednym z wymagań, które obowiązuje administratorów przetwarzających takie dane, jest zapewnienie pełnej rozliczalności dotyczącej operacji przetwarzania. Ogólnie obowiązująca zasada rozliczalności w kontekście posiadania uprawnień dostępu do danych rozumiana jest jako zapewnienie informacji o tym, kto dane wprowadził, zmienił lub wykasował. Nie obejmuje ona np. operacji przeglądania danych, do przetwarzania których użytkownik systemu posiada upoważnienie. W odniesieniu natomiast do dokumentacji medycznej obowiązek rozliczalności został rozszerzony również w zakresie dotyczącym tylko wglądu do informacji.

Ważne jest więc przede wszystkim dopasowanie uprawnień do roli pracownika, a także zarządzanie tymi uprawnieniami. Bezpieczeństwo nie polega na tym, że uprawnienia te raz się ustanawia, a potem wszystko funkcjonuje bez problemu. Bezpieczeństwo trzeba monitorować, śledzić, a nadane uprawnienia co jakiś czas weryfikować, sprawdzać, czy np. w związku ze zmianą stanowiska lub zakresu obowiązków uprawnienia nadane kiedyś wciąż są odpowiednie. Kierownik danej jednostki czy pracownik zwraca się zazwyczaj o stosowne zmiany, gdy uprawnień ma za mało, gdy nie pozwalają one mu wykonywać powierzonych zadań. Rzadko natomiast użytkownicy zgłaszają przypadki wskazujące na nadmiar posiadanych uprawnień. Stąd ważnym elementem nadzoru nad przetwarzaniem danych medycznych jest systematycznie monitorowanie nadanych uprawnień.

Co zmieni w tym zakresie RODO?

Obecnie obowiązujące przepisy dosyć rygorystycznie określają, jak należy zarządzać uprawieniami dostępu do danych. Wymagane jest prowadzenie ewidencji osób upoważnionych do przetwarzania danych, wskazana jest też wymagana zawartość informacji, jaką ona powinna zawierać itd. Przepisy określają również zakres wymaganej dokumentacji przetwarzania danych, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wskazuje minimalne wymagania w zakresie środków bezpieczeństwa, jakie należy zastosować w zależności od kategorii danych oraz ogólnych informacji o środowisku, w jakim dane osobowe są przetwarzane.

Przepisy rozporządzenia Ministra Administracji i Cyfryzacji z 11.05.2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji określają również zadania, jakie ma realizować administrator bezpieczeństwa informacji w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych. Wskazują one nawet sposób dokumentowania tych czynności.

RODO nie daje w powyższym zakresie żadnych szczegółowych rozwiązań. Nie określa, w jaki sposób powinna być prowadzona dokumentacja przetwarzania danych osobowych, nie wskazuje, jakie elementy powinny być zawarte w polityce bezpieczeństwa czy instrukcji zarządzania systemem informatycznym. Nie ustanawia również żadnych minimalnych wymagań odnoszących się do sposobu zabezpieczenia przetwarzanych informacji.

RODO nie daje w powyższym zakresie żadnych gotowych rozwiązań, żadnych propozycji odnośnie do ich dokumentowania, a nawet propozycji w zakresie ich jakości. Administratorom danych zapewnia pod tym względem ogromną swobodę. Stawia jedynie pewne ogólne wymagania odnoszące się do bezpieczeństwa przetwarzanych danych, wskazując cele, jakie w ich wyniku powinny być uzyskane.

Artykuł 24 RODO zobowiązuje administratorów danych, aby uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdrożyli odpowiednie środki techniczne i organizacyjne, które zapewnią zgodność przetwarzania z rozporządzeniem. Zwraca jednocześnie uwaga na to, aby możliwe było ich wykazanie, co należy rozumieć jako formalne ich udokumentowanie.

RODO daje jedynie sugestie dotyczące wbudowania pewnych elementów zwiększających bezpieczeństwo przetwarzania danych w projekt przetwarzania danych. Stanowi o tym art. 25 RODO, w którym sugeruje się podnoszenie poziomu bezpieczeństwa poprzez uwzględnianie potrzeb w zakresie ochrony danych już w fazie projektowania systemu oraz stosowania takich rozwiązań organizacyjnych, które domyślnie dają uprawnienia do minimalnego zakresu danych. Ustępy 1 i 2 powołanego przepisu wskazują odpowiednio, że:

- administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą, oraz

- administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Do środków takich można zaliczyć np. mechanizm sprawdzający, czy dane odpowiadające dacie urodzenia są zgodne z formatem danych, czy mechanizm, który przy wklejaniu numeru konta do formatki przelewu środków automatycznie zmieni ostatnie cyfry tego numeru na znaki * lub ?, aby zwrócić uwagę operatora i wymusić jego weryfikację.

W praktyce oznacza to, że każda placówka musi sama określić ryzyko, na jakie narażone są przetwarzane dane i określić zarówno środki organizacyjne, jak i techniczne, które zapewnią odpowiedni poziom bezpieczeństwa.

Jak wyglądają te działania w dużych szpitalach, a jak w małych placówkach?

Skuteczność systemu zabezpieczenia zależy od tego, ile słabych punktów występuje w danym procesie przetwarzania i czy wszystkie zostały zidentyfikowane oraz odpowiednio zabezpieczone. Skuteczność całego systemu bezpieczeństwa zależy bowiem od najsłabszego ogniwa w całym łańcuchu czynności przetwarzania. Im system jest większy, tym tych punktów (ogniw) jest więcej. Na przykład w szpitalu, gdzie mamy wiele stacji roboczych, serwerów, urządzeń laboratoryjnych, które są podłączone do Internetu i są widziane w sieci publicznej, występuje przesyłanie informacji między nimi - tych punktów zagrożeń dla bezpieczeństwa może być bardzo dużo. Ich identyfikacja i wprowadzenie odpowiednich mechanizmów kontrolnych łagodzących skutki ich zaistnienia bądź eliminujących ich zaistnienie wymaga przeprowadzenia analizy ryzyka wg schematu, w którym analizowane są kolejno wszystkie potencjalne zagrożenia. Dla dużych organizacji, w których korzysta się z wielu różnych systemów, gdzie występuje wiele przepływów danych pomiędzy systemami, gdzie korzysta się z usług zewnętrznych, warto jest rozważyć przeprowadzenie profesjonalnej analizy oceny ryzyka opartej o określoną metodykę, co zapewni jej kompletność. Możliwe jest np. przeprowadzenie oceny ryzyka zgodnie z metodyką przedstawioną w normie ISO/IEC 27005 oraz wdrożenie zabezpieczeń wg zaleceń normy ISO/IEC 27002.

W przypadku pojedynczego gabinetu, ze względu na mniejszą złożoność systemu przetwarzania (pojedynczy komputer oraz jedno lub kilka specjalistycznych urządzeń) elementów stanowiących istotne zagrożenie dla bezpieczeństwa informacji jest mniej. Trzeba wówczas podejść do zagadnienia w taki sam sposób, jak w dużej placówce, ale w mniejszym zakresie – uwzględniać tylko te elementy wprowadzające ryzyko, które rzeczywiście występują. W przypadku prywatnego gabinetu lekarskiego, w którym przyjmuje tylko jeden lekarz, nie pojawia się problem zarządzania uprawnieniami. Wystarczy wówczas zainstalować system antywirusowy, zabezpieczyć dostęp do danych przetwarzanych na komputerze poprzez wprowadzenie kontroli dostępu (identyfikator i hasło) oraz zapewnić fizycznie ochronę pomieszczenia (gabinetu) m.in. poprzez zabezpieczenie okien (kraty czy folię antywłamaniową – jeśli występuje taka potrzeba) i zamykanie drzwi po opuszczeniu gabinetu.

Jak należy dbać o bezpieczeństwo danych w przypadku, gdy używa się rozwiązań w zakresie telemedycyny?

W przypadku telemedycyny należy odpowiednio konstruować system teleinformatyczny, który będzie służył do przekazywania i wstępnej analizy danych medycznych, a także niezbędnych w takich systemach komunikatów dla użytkownika (pacjenta), lekarza czy placówki medycznej. Istnieją różne metody zabezpieczenia danych, na przykład pseudonimizacja. Warto pamiętać, że wówczas, gdy chcemy konsultować jakiś obraz czy wynik badania, wystarczy przesłać je bez danych osobowych pacjenta, a jedynie z danymi, które są konieczne do oceny wyniku badania, takimi jak np. wiek czy stan zdrowia, inne dolegliwości itd.

Jeśli już rozmawiamy o telemedycynie, warto też wspomnieć o tym, że coraz częściej sami pacjenci korzystają z urządzeń analizujących stan ich zdrowia, na przykład pracę serca czy poziom cukru we krwi, i przesyłających wyniki zdalnie do centrum monitoringu. W tym przypadku należy uwzględniać fakt, że osoby te mogą zostać zidentyfikowane poprzez dane identyfikujące urządzenie. Do identyfikacji takiej mogą być wykorzystane dane dotyczące ruchu telekomunikacyjnego, jaki towarzyszy takiemu przekazywaniu danych. Dane takie zapamiętywane są zazwyczaj przez operatora sieci, z usług którego korzystamy, który zna nasze dane identyfikacyjne. W sytuacji takiej mechanizmy pseudonimizacji mogą okazać się bezskuteczne i niezbędne będzie zastosowanie rozwiązań kryptograficznych.

Podobne problemy dotyczą ochrony danych, jakie przesyłane są przez indywidualnie wykorzystywane urządzenia medyczne i urządzenia używane przez sportowców podczas treningów, które poza takimi danymi, jak czas i szybkość poruszania się, dokonują pomiaru wielu innych parametrów naszego organizmu, takich jak tętno, ciśnienie itp., które w połączeniu ze sobą mogą zawierać istotne informacje o stanie naszego zdrowia. Dane takie często nie tylko zapisywane są na urządzeniu, które jest pod naszą kontrolą, ale również na serwerach dostawcy danej usługi lub w dzierżawionej przez niego chmurze obliczeniowej.

Niezwykle szybki postęp technologiczny, z jakim mamy do czynienia w ostatnich latach, powodował, że prawo nie nadążało z regulowaniem wszystkich aspektów przetwarzania danych przy użyciu nowoczesnych metod. Jeszcze trudniej byłoby przewidzieć, jakie usługi i mechanizmy przetwarzania powstaną w najbliższej przyszłości, jakie będą związane z nimi zagrożenia dla prywatności i ochrony danych oraz jakie stosować narzędzia, aby ograniczać lub eliminować potencjalne skutki tych zagrożeń.

Dlatego RODO nie zawiera ścisłych wskazówek odnoszących się do każdej sytuacji przetwarzania danych z wykorzystaniem nowoczesnych rozwiązań technologicznych. Wymaga natomiast, aby każdy przypadek poddawany był analizie z punktu widzenia ryzyk, jakie dane rozwiązanie może powodować dla ochrony naszych danych. Jednocześnie zwraca uwagę, aby w analizie takiej uwzględniać stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

Coraz powszechniejsze są rozwiązania polegające na tworzeniu portali pacjenta, umożliwiających rejestrację czy dostęp do wyników badań przez Internet, lub nawet chatów z lekarzami. Na co należy zwracać uwagę przy wprowadzaniu takich rozwiązań?

Takie systemy trzeba także przeanalizować pod kątem stosowanych w nich zabezpieczeń. Duże firmy częściej korzystają ze sprawdzonych rozwiązań, ale przestrzegałbym - szczególnie małe gabinety - przed stosowaniem w tym zakresie technologii, która nie jest przystosowana do przetwarzania informacji związanych ze stanem zdrowia pacjentów. Na rynku dostępnych jest wiele narzędzi, które są przydatne do komunikacji bezpośredniej, ale trzeba sprawdzić, czy są one należycie zabezpieczone przed atakami i czy należycie zabezpieczają dane.

Zdarza się, że narzędzia tego typu dostarczane są przez tzw. domowych programistów, czasem tworzone są w ramach eksperymentu, którego celem jest osiągnięcie konkretnego rozwiązania. Nie zawsze jednak sposób, w jaki cel ten osiągnięto, jest bezpieczny. Nie zawsze przetwarzane w tym celu dane zabezpieczone są przed wykorzystaniem ich w innym celu. Nie zawsze również przetwarzane przy użyciu takich programów dane są odpowiednio zabezpieczone przed dostępem osób nieupoważnionych. Być może tego typu rozwiązania mogą być tańsze, ale nie zawsze bezpieczne.

Natomiast w przypadku korzystania z chmury obliczeniowej należy zadbać o właściwą izolację danych w chmurze.

Przykładem może być glukometr oraz towarzysząca mu aplikacja mobilna, które były przedmiotem badań GIODO. Wykazały one, że użytkownik badanego glukometru może pobrać ze strony internetowej jego producenta aplikację, za pośrednictwem której dane zbierane przez to urządzenie mogą być dalej przetwarzane. Aplikacja ta zainstalowana na smartfonie użytkownika umożliwia bowiem - oprócz prezentacji statystyk dla zbieranych danych - także przechowywać je na dysku w chmurze obliczeniowej, z której właścicielem producent glukometru podpisał umowę.

Z przeprowadzonych przez Biuro GIODO badań tego glukometru wynikało, że procesy przekazywania danych zostały dokładnie opisane w instrukcjach, z którymi użytkownik zobowiązany był zapoznać się w czasie instalacji aplikacji. Instrukcje te wyraźnie wskazywały, że zainstalowanie i wykorzystywanie tej aplikacji równoznaczne jest z wyrażeniem zgody na pobieranie tych danych i zapamiętywanie ich w dzierżawionym obszarze konkretnie wskazanej chmury obliczeniowej.

Czy RODO zawiera szczegółowe regulacje dotyczące outsourcingu?

Przepisy dotyczące przetwarzania danych medycznych do 12.12.2015 r. w ogóle wyłączały możliwość outsourcingu przetwarzania danych, m.in. przez podmioty świadczące usługi informatyczne. Przesądzały one bowiem, że do przetwarzania danych medycznych uprawnione są tylko osoby z uprawnieniami medycznymi lub wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych. Przepisy te zmieniono dopiero ustawą z 9.10.2015 r. o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw, w której zmieniono art. 24, zapisując w jego ust. 2, że dostęp do dokumentacji mogą mieć ponadto osoby wykonujące czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i z zapewnieniem bezpieczeństwa tego systemu. Dostęp taki może być nadawany wyłącznie w drodze upoważnienia przez administratora danych. Osoby, którym upoważnienie takie zostanie wydane, zobowiązane są do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z wykonywaniem zadań. Przy czym tajemnica ta obowiązuje również po śmierci pacjenta.

RODO nie zawiera takiego ograniczenia. Prawo krajowe może jednak doprecyzować postanowienia RODO w tym zakresie, o czym stanowi jego art. 9 ust. 4.W przypadku outsourcingu RODO wyraźnie jednak podkreśla, że przetwarzanie takie może się odbywać, ale wyłącznie zgodnie z poleceniami administratora danych. Oznacza to, że w umowie powierzenia przetwarzania musi być dokładnie określony zakres tego przetwarzania, czyli – w jakim zakresie się ono odbywa i jakie operacje mogą być wykonywane na tych danych.

Wyraźnie jednak wpływ na prawa i obowiązki obu stron ma przyjęta w unijnym rozporządzeniu tzw. zasada rozliczalności, zgodnie z którą zarówno administrator, jak i podmiot przetwarzający muszą wykazać przestrzeganie nowego prawa (np. poprzez udokumentowane wdrożenie instrumentów prawnych określonych w rozporządzeniu, takich jak m.in. przeprowadzona ocena skutków dla ochrony danych).

Zgodnie z tą nową filozofią, administrator, który powierza przetwarzanie danych, będzie musiał przy wyborze podmiotu przetwarzającego (tj. podmiotu, któremu dane zostają powierzone) samodzielnie ocenić, czy podmiot ten zapewnia właściwą ochronę powierzanych danych, co powinno być elementem analizy i szacowania ryzyka. Zgodnie bowiem z art. 28 ust. 1 RODO, jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzystać on musi wyłącznie z usług takich podmiotów przetwarzających, które zapewnią wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Swego rodzaju nowością jest również wyraźne wskazanie (w art. 28 ust. 2 RODO), że podmiot przetwarzający nie będzie mógł korzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku zaś ogólnej pisemnej zgody, podmiot przetwarzający będzie musiał poinformować administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

W przepisach RODO wyraźnie określono też (art. 28 ust. 3 lit. g), że po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji administratora, podmiot przetwarzający usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

W kontekście RODO warto też wspomnieć o nowych obowiązkach podmiotu przetwarzającego, do których zaliczyć należy:

- pomaganie (w miarę możliwości) administratorowi, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO,

- pomaganie administratorowi w wywiązaniu się z obowiązków określonych w art. 32–36 RODO, takich jak: zapewnianie bezpieczeństwa przetwarzania, zgłaszanie naruszeń ochrony danych organowi nadzorczemu, informowanie osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych, a więc np. o wycieku danych, a także przeprowadzaniu oceny skutków dla ochrony danych.

Reasumując, RODO doprecyzowuje wzajemne relacje między administratorem a podmiotem przetwarzającym z uwzględnieniem nowych instrumentów zapewniających wykazanie zgodności, takich jak np. szacowanie ryzyka czy zgłaszanie naruszeń.

Szpitale i inne jednostki z sektora ochrony zdrowia muszą zatem przejrzeć umowy z podmiotami, które przetwarzają dla nich dane, i sprawdzić, czy spełniają one wymagania, które wynikają z RODO.

Gdzie można szukać wiedzy na temat bezpieczeństwa informacji?

Cała baza wiedzy, która dotyczy bezpieczeństwa informacji, zawarta jest w różnego rodzaju dobrych praktykach, przewodnikach czy też normach krajowych, europejskich bądź międzynarodowych. W odniesieniu do bezpieczeństwa informacji w sektorze medycznym na szczególna uwagę zasługują normy z serii ISO/IEC 27000 dotyczące bezpieczeństwa danych przetwarzanych w systemach teleinformatycznych oraz normy ściśle związane z przetwarzaniem danych medycznych, jak np. ISO/TS 17090 - Informatyka w ochronie zdrowia – Infrastruktura klucza publicznego, PN-ENV 13606 - Przesyłanie elektronicznego rekordu medycznego czy PN-ENV 13608 - Informatyka zdrowotna – Bezpieczeństwo przesyłania danych w opiece zdrowotnej.

W wielu przypadkach wymagania z tych norm przenoszone są do przewodników, tzw. dobrych praktyk, stosowanych przez administratorów danych lub wprost do przepisów prawa. Na przykład rozporządzenie Rady Ministrów z 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, oprócz elementów związanych z interoperacyjnością, czyli z możliwością współdziałania systemów i wymiany informacji między systemami, zawiera rozdział, który dotyczy bezpieczeństwa przetwarzania danych i odpowiedniego zabezpieczenia systemu informatycznego. Zawarte w nim wymagania dotyczące bezpieczeństwa danych przetwarzanych w systemach informatycznych są w dużej części odzwierciedleniem wymagań zawartych w normie PN-ISO/IEC 27001.

Żeby zapewnić bezpieczeństwo danych przetwarzanych przy użyciu systemów teleinformatycznych ważne jest przede wszystkim, aby używane do tego przetwarzania systemy były bezpieczne. Żeby z kolei skutecznie zabezpieczyć system teleinformatyczny, trzeba mieć wiedzę o wszystkich jego składnikach, występujących pomiędzy nimi przepływach danych, a także wykorzystywanych w tym celu protokołach komunikacyjnych. Potrzebna jest zatem pełna inwentaryzacja posiadanych urządzeń i programów, a także ich konfiguracji. Zabezpieczenie danych przetwarzanych w systemach teleinformatycznych wymaga odpowiedniego zabezpieczenia każdego elementu, modułu programowego, w którym dane te są przetwarzane, a także każdego przepływy tych danych między nimi. Wymaga się tam również, aby system zapewniał kontrolę dostępu do przetwarzanych danych i aby organizacyjnie zapewnić, że dostęp taki posiadają tylko osoby, którym on jest niezbędny do realizacji ich zadań. Od administratorów systemu wymaga się z kolei, aby właściwie dbali o bezpieczeństwo systemu poprzez m.in. ich ciągłe monitorowanie, dokonywanie przeglądów, aktualizację oprogramowania, a także zabezpieczeń przed nieuprawnioną ich modyfikacją. Wymaga się również, aby administratorzy systemów dbali o zapewnienie bezpieczeństwa plików systemowych, zastosowanie mechanizmów ochrony kryptograficznej – jeśli informacje przekazywane są za pośrednictwem sieci publicznej, a także zapewniali ochronę przed kradzieżą danych, nieuprawnionym wykorzystaniem, dostępem lub uszkodzeniem.

Rozmowa i opracowanie: Magdalena Okoniewska

Data publikacji: 18 grudnia 2017 r.

Inspektor Ochrony Danych(z ang. Data protection officer – DPO)

Nowa ustawa o ochronie danych osobowych jest w trakcie przygotowania, dlatego wytyczne krajowe nie są jeszcze znane. W obowiązującym stanie prawnym (ustawa o ochronie danych osobowych) istnieje konieczność zgłaszania do GIODO informacji o powołaniu lub odwołaniu administratora bezpieczeństwa informacji (w terminie 30 dni od powołania/ odwołania). RODO nie stawia przed administratorem danych takich obowiązków, jednak nie wyznaczenie inspektora tam, gdzie jest taka konieczność, stanowi naruszenie przepisów, co po 25 maja 2018 roku będzie podlegać administracyjnym karom pieniężnym w wysokości do 10 mln euro, a w przypadku przedsiębiorstw nawet do 2% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego (jeżeli te 2% wynosi mniej niż 10 mln euro, to w dalszym ciągu można nałożyć na przedsiębiorstwo karę do 10 mln euro).

Rozporządzenie przewiduje obligatoryjne wyznaczenie inspektora w sytuacji gdy:

- przetwarzania dokonują organ lub podmiot publiczny,
- główna działalność administratora lub procesora polega na operacjach przetwarzania, które ze względu na swój charakter, zakres, lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę,
- **główna działalność administratora lub procesora polega na przetwarzaniu na dużą skalę danych osobowych szczególnych kategorii (np. o stanie zdrowia**) oraz danych o wyrokach skazujących za przestępstwa. Należy zaznaczyć, iż przetwarzanie danych osobowych nie powinno być uznane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika.

Państwo członkowskie może przewidzieć inne sytuacje, w których będzie powołany obligatoryjnie inspektor. Na chwilę obecną nie wiadomo czy Polska skorzysta z takiej możliwości.

Dodatkowe trudności wprowadza samo RODO, które dokładnie precyzuje, jakie cechy musi posiadać osoba pełniąca funkcję IOD. Wiedza merytoryczna i znajomość przepisów prawa nie będzie wystarczająca. „Nowy ABI" będzie musiał posiadać także doświadczenie z zakresu ochrony danych osobowych, czyli praktyczną umiejętność realizacji zadań (np. prowadzenia kontroli i szkoleń, umiejętności oceny zabezpieczeń oraz redagowania procedur) i znać branżę, z którą pracuje. Niezbędna będzie także znajomość technologii oraz stosowanych przez organizację rozwiązań informatycznych.

RODO wzmacnia pozycję IOD

Inspektor ochrony danych będzie pełnił funkcje obecnego ABI, ale rozporządzenie o ochronie danych osobowych jasno wskazuje, jakie warunki musi spełniać osoba powołana na to stanowisko (art. 38 RODO):

Inspektor ochrony danych, tak jak dotychczas ABI, podlegać będzie bezpośrednio najwyższemu kierownictwu administratora oraz za prawidłowe wypełnianie swoich zadań inspektor nie będzie mógł być przez administratora karany ani odwołany. Co ważne, administrator zobowiązany będzie do terminowego i właściwego angażowania inspektora we wszystkie sprawy dotyczące ochrony danych osobowych.

Inspektor ochrony danych i jego zadania

Rozporządzenie o ochronie danych osobowych mówi, jakie konkretne zadania musi wykonywać IOD (art. 39 RODO):

1. **informowanie** administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów, a także doradzanie im w tej sprawie.
2. dawanie **wskazówek administratorowi** w przedmiocie wdrożenia odpowiednich i skutecznych środków technicznych a także organizacyjnych mających zabezpieczyć dane osobowe. Ponadto wykazanie przestrzeganie prawa przez administratora lub podmiotu przetwarzającego dane zwłaszcza w kwestiach związanych z identyfikowaniem ryzyka dotyczącego ochrony danych, jego ocenę oraz wyznaczenie praktyk pozwalających zminimalizować to ryzyko.
3. **monitorowanie przestrzegania** rozporządzenia oraz innych przepisów obowiązujących w Unii lub państwach członkowskich o ochronie danych, polityk administratora, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.
4. **udzielanie na żądanie zaleceń co** do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania.
5. współpraca z organem nadzorczym oraz **pełnienie funkcji punktu kontaktowego** dla organu nadzorczego w kwestiach związanych z przetwarzaniem oraz w stosownych przypadkach prowadzenie konsultacji we wszystkich innych sprawach.
6. inspektor ochrony danych ma stać się nie tylko punktem kontaktowym **dla GIODO, ale również dla osób, których dane dotyczą**, we wszystkich kwestiach związanych z przetwarzaniem ich danych osobowych oraz sprawach dotyczących przysługujących im uprawnieniom.

   Inspektor ochrony danych będzie miał dużo więcej obowiązków niż dotychczasowy ABI, ale również więcej praw. Należy jednak pamiętać, że to administrator danych osobowych będzie ponosił największą odpowiedzialność za przestrzeganie przepisów RODO. Dlatego tak ważne jest wybranie odpowiedniego inspektora i stworzenie mu jak najlepszych warunków do wykonywania powierzonych zadań.

Inspektor ochrony danych będzie pełnił funkcje obecnego ABI, ale rozporządzenie o ochronie danych osobowych jasno wskazuje, jakie warunki musi spełniać osoba powołana na to stanowisko (**art. 38 RODO**):

1. inspektor musi podlegać bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego,
2. administrator oraz podmiot przetwarzający zapewniają, by inspektor był właściwie i niezwłocznie włączony we wszystkie sprawy dotyczące ochrony danych osobowych,
3. administrator oraz podmiot przetwarzający zapewniają, by IOD nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,
4. **inspektor nie może być karany ani odwołany przez administratora lub przetwarzającego dane za wypełnianie swoich zadań,**
5. inspektor jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywanych swoich zadań,
6. inspektor może wykonywać inne zadania i obowiązki, pod warunkiem, że nie powodują one konfliktu interesów.

Nowością przewidzianą w rozporządzeniu jest możliwość wyznaczenia jednego inspektora danych przez grupę grupa przedsiębiorców oraz przez organy lub podmioty publiczne. Jednakże należy ostrożnie podchodzić do wyznaczenia jednego inspektora ochrony danych w szczególności dla kilku podmiotów publicznych, gdyż może to powodować fikcyjny nadzór nad systemem ochrony danych w tych podmiotach.

Status DPO w praktyce

DPO musi być włączany we wszystkie etapy działań związanych z przetwarzaniem danych osobowych podejmowanych przez przedsiębiorcę oraz musi być terminowo powiadamiany o wszystkich kwestiach dotyczących przetwarzania danych osobowych. Poza tym DPO:

1) w strukturze organizacyjnej przedsiębiorcy podlega bezpośrednio najwyższemu kierownictwu administratora lub procesora,

2) zachowuje w tajemnicy lub poufności szczegóły wykonywanych zadań,

3) może wykonywać inne zadania i obowiązki, o ile nie generują konfliktu interesów,

4) mogą kontaktować się z nim osoby, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia.

Obowiązki ADO oraz podmiotu przetwarzającego (procesora)

Przedsiębiorca, u którego działa DPO, jest obowiązany zapewnić wszelkie niezbędne środki, których DPO potrzebuje do wykonywania swojej pracy, takie jak: przestrzeń biurowa, pracownicy, sprzęt elektroniczny itp. Poza tym przedsiębiorcy:

1) zapewniają udział DPO w sprawach związanych z ochroną danych osobowych,

2) zapewniają DPO odpowiednie narzędzia i dostęp do danych osobowych niezbędnych do wykonywania zadań,

3) **umożliwiają DPO aktualizowanie wiedzy fachowej,**

4) dbają by jego inne zadania i obowiązki nie generowały konfliktu interesów,

5) nie instruują DPO odnośnie wykonywania zadań z ochrony danych osobowych,

6) **nie mogą odwołać ani karać DPO za wykonywanie jego zadań.**