

Inspektor ochrony danych obowiązkowy w szpitalach

data: 06-11-2017

Dla menedżerów

Od 25 maja 2018 roku, czyli od dnia, w którym zaczniemy w Polsce stosować unijne ogólne rozporządzenie o ochronie danych osobowych, wszystkie publiczne placówki medyczne będą musiały zatrudniać inspektorów ochrony danych (dziś nazywanych administratorami bezpieczeństwa informacji, w skrócie ABI). W przypadku większości szpitali prywatnych obowiązek ten będzie wynikał z faktu, że główna działalność szpitali wymaga przetwarzania danych o stanie zdrowia na dużą skalę.

GRC Zarządzanie RODO



Monika Młotkiewicz

Na pytania odpowiada Monika Młotkiewicz, zastępca dyrektora Departamentu Rejestracji Administratorów Bezpieczeństwa Informacji i Zbiorów Danych Osobowych w Biurze Generalnego Inspektora Ochrony Danych Osobowych (GIODO)

Przepisy dotyczące inspektorów ochrony danych osobowych to u nas nie nowość...

Tak, jesteśmy w Polsce w korzystnej sytuacji, gdyż przepisy ustawy o ochronie danych osobowych dotyczące ABI uległy dużej zmianie z początkiem 2015 roku i obecnie są bardzo zbliżone do tych uregulowań, które zawiera unijne rozporządzenie w stosunku do inspektorów ochrony danych.

Inspektorzy ochrony danych osobowych - tak jak teraz ABI - będą musieli wykazywać się odpowiednią wiedzą w dziedzinie ochrony danych, wykonywać swoją funkcję w sposób niezależny oraz podlegać bezpośrednio kierownictwu placówki.

Niemniej przepisy rozporządzenia dotyczące inspektorów ochrony danych jeszcze bardziej wzmacniają pozycję tych osób, dają im więcej gwarancji niezależności. Zmieniają też katalog zadań inspektora, rozszerzając go o pewne nowe obowiązki.

Zmiana ustawy o ochronie danych osobowych dała polskim podmiotom szansę na solidne, stopniowe dostosowanie się do nowych wspólnotowych przepisów. Te 3,5 roku - od początku 2015 roku do prawie połowy 2018 roku, to był czas na to, aby wyszukać odpowiednią osobę na to stanowisko i wesprzeć ją w podnoszeniu kwalifikacji. Dzięki temu można było zyskać fachowca, który pomoże przygotować całą organizację do stosowania unijnej regulacji.

Czy placówki dobrze wykorzystały ten czas?

Niektóre na pewno tak. Ale są też takie podmioty, które nie mają swojego administratora bezpieczeństwa informacji i w związku dostosowanie do nowych wymogów będzie dla nich trudniejszym zadaniem.

W tej chwili polskie prawo nie przewiduje obowiązku wyznaczania ABI. Założenie tego rozwiązania było takie, że na pełnienie tej funkcji decydować się powinny tylko osoby posiadające odpowiednie merytoryczne przygotowanie do pełnienia tej funkcji. Taki stan prawny – jak już wspomniałam - będzie obowiązywał do 25 maja 2018 roku. Po tej dacie na większości szpitali - w tym szpitali przekształconych w spółki z udziałem samorządów wojewódzkich, powiatowych czy gminnych, klinik i przychodni - będzie spoczywał obowiązek posiadania takiej osoby.

Kto będzie musiał zatrudnić inspektora ochrony danych?

Tak jak wspomniałam, obowiązek ten będzie dotyczył wszystkich podmiotów publicznych, a więc publicznych szpitali, klinik i przychodni, w tym tych przekształconych w spółki z udziałem samorządów wojewódzkich, powiatowych czy gminnych. Obowiązek ten będzie też dotyczył większości placówek prywatnych, ponieważ przepis rozporządzenia stanowi, że do wyznaczenia inspektora ochrony danych zobowiązane są między innymi te podmioty, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, a do takiej kategorii należą dane o stanie zdrowia.

Być może sposób sformułowania przepisu określającego obowiązek wyznaczenia inspektora jest mało precyzyjny, ale takie sformułowanie zostało użyte celowo, właśnie po to, aby administratorzy danych samodzielnie dokonywali analizy sytuacji i oceniali, czy taki obowiązek w ich przypadku istnieje.

W celu ułatwienia im tego zadania, Grupa Robocza Artykułu 29 - organ doradczy Komisji Europejskiej w zakresie ochrony danych osobowych i prywatności, w skład którego wchodzi unijni rzecznicy ochrony danych, a więc także Generalny Inspektor Ochrony Danych Osobowych - od pewnego czasu opracowuje wyjaśnienia do wielu przepisów rozporządzenia. W połowie grudnia 2016 roku wydała Wytyczne dotyczące inspektorów ochrony danych.

Wytyczne te zawierają wskazówki, jak należy rozumieć „główną działalność” czy „dużą skalę”, a także wiele praktycznych, konkretnych przykładów sytuacji spełniających te kryteria. W Wytycznych zaznaczono, że w przypadku placówek medycznych główną działalnością jest wprawdzie zapewnianie opieki zdrowotnej, ale ta działalność nie byłaby możliwa bez przetwarzania danych w formie dokumentacji medycznej. Dlatego jako przykład działalności głównej polegającej na przetwarzaniu na dużą skalę wrażliwych danych osobowych jest tam podana właśnie działalność szpitali.

Warto dodać, że w tym samych sytuacjach RODO przewiduje obowiązek wyznaczenia inspektora ochrony danych przez tzw. podmioty przetwarzające, czyli podmioty, które przetwarzają dane osobowe na zlecenie placówek medycznych w związku ze specjalistycznymi usługami, jakie dla nich świadczą, na przykład przechowują dokumentację medyczną lub serwisują sprzęt informatyczny czy diagnostyczny.

A co z przychodniami? Są przecież niewielkie placówki zatrudniające na przykład dwóch lekarzy i dwie pielęgniarki. Czy one także muszą zatrudniać inspektora ochrony danych?

Nikt nie udzieli odpowiedzi na to pytanie bez dokładnej analizy konkretnej sytuacji. Taką ocenę powinien przeprowadzić każdy podmiot we własnym zakresie. Co więcej – we wspomnianych Wytycznych zaleca się, aby przeprowadzenie oceny w zakresie istnienia obowiązku wyznaczenia inspektora udokumentować, a nawet powtarzać taką ocenę w razie potrzeby, co jakiś czas, gdyż sytuacja danego podmiotu może się zmieniać. Na przykład mała przychodnia może stopniowo rozszerzać swoją działalność, obejmując nią nowe usługi i świadczenia i po jakimś czasie stać się dużym podmiotem przetwarzającym dane wrażliwe na dużą skalę. W przypadku indywidualnej praktyki lekarskiej czy gabinetu prowadzonego przez lekarza, racjonalnie można przyjąć, że nie ma tutaj mowy o działalności na dużą skalę i dlatego taki lekarz nie będzie miał obowiązku zatrudniać inspektora ochrony danych.

Motyw 91 rozporządzenia, który dotyczy wprawdzie obowiązku prowadzenia oceny skutków działalności dla ochrony danych osobowych, ale też odnosi się do pojęcia dużej skali, podaje przykłady pojedynczych prawników i lekarzy jako te sytuacje, kiedy nie ma obowiązku zatrudniania inspektora ochrony danych.

Nowe przepisy dają większą elastyczność w interpretacji...

W przepisach rozporządzenia ogólnego jest zawarta pewna elastyczność. Ten akt prawny nie przynosi rewolucji w zakresie zasad i uprawnień osób, których dane dotyczą; tutaj mamy raczej ewolucję, wzmocnienie dotychczasowego dorobku. Rewolucja dokonuje się natomiast w zakresie podejścia do stosowania i egzekwowania prawa. Ta rewolucja polega między innymi na tym, że w wielu przypadkach sami dokonujemy oceny, czy dany przepis nas dotyczy i w jaki sposób powinniśmy go zastosować.

Z jednej strony oznacza to większą elastyczność i swobodę w doborze rozwiązań, ale z drugiej – większą samodzielność i odpowiedzialność. Będzie obowiązywała zasada rozliczności, wymuszająca gotowość udowodnienia, że przyjęte przez organizację rozwiązania są zgodne z prawem i skuteczne. Rozporządzenie ogólne wymaga zatem, aby stosować takie rozwiązania i środki w zakresie przetwarzania danych osobowych, które

odpowiadają różnym, skonkretyzowanym potrzebom i zagrożeniom, sprawdzą się, zadziałają w różnorodnych, realnych sytuacjach. Takie podejście ma na celu urzeczywistnienie zasad ochrony.

Dotychczas działania związane z ochroną danych osobowych sprowadzały się często jedynie do spełnienia wymogów formalnych, do opracowywania zestawu dokumentacji według jednego uniwersalnego wzoru. Często taka dokumentacja i zasady w niej określone nie były znane i stosowane przez ogół pracujących w danej instytucji osób, co sprawiało, że ochrona danych osobowych w niektórych podmiotach była fikcją.

To nowe podejście, ta konieczność dokonywania analizy i oceny, jakie rozwiązania należy zastosować, aby być w zgodzie z nowymi przepisami o ochronie danych osobowych, będzie prawdopodobnie powodować, że bardzo wiele podmiotów - nawet tych, które nie są zobowiązane do wyznaczenia inspektora ochrony danych - będzie chciało z pomocy takiej osoby korzystać. Obecnie dostępne metody przetwarzania i zabezpieczenia danych są coraz bardziej złożone, dlatego osoba posiadająca na ten temat specjalistyczną wiedzę może stanowić znaczące, wręcz niezbędne wsparcie dla osób zarządzających placówkami medycznymi. Zwłaszcza że w sektorze opieki zdrowotnej szczególnie ważna jest dbałość o poszanowanie prawa do ochrony danych osobowych i prywatności pacjentów. Niezgodne z zasadami przetwarzania danych wrażliwych może spowodować nie tylko poważne skutki finansowe i prawne dla placówki medycznej, ale przede wszystkim bardzo dotkliwe i trudne do zaakceptowania krzywdy i szkody dla osób, których dane dotyczą. Dla pacjentów wszelkie naruszenia tajemnicy, jaką objęte są dane związane z korzystaniem przez nich z usług medycznych, mogą skłaniać ich do wystąpienia z roszczeniami czy skargą do odpowiednich organów, w tym GIODO.

Jakie wymagania musi spełniać inspektor ochrony danych?

Osoba taka musi przede wszystkim mieć dobre merytoryczne przygotowanie do pełnienia tej funkcji. Musi dysponować fachową wiedzą i ma to być wiedza na temat prawa i praktyk w dziedzinie ochrony danych osobowych. Zatem liczy się nie tylko wiedza teoretyczna, ale też umiejętności jej praktycznego zastosowania, co najczęściej wynika z doświadczenia zawodowego.

Dlatego wyboru odpowiedniej osoby na to stanowisko należy dokonywać starannie. Wymagany od inspektora poziom wiedzy fachowej nie jest nigdzie jednoznacznie określony, ale zgodnie ze wspomnianymi wytycznymi Grupy Roboczej Art. 29, musi być on współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w danej jednostce. Podobnie jak w wielu innych dziedzinach, gdzie nie obowiązuje system egzaminów państwowych, pomocne w dokonywaniu oceny kwalifikacji takiej osoby mogą być wszelkie przedstawiane przez nią dowody poświadczające jej fachową wiedzę i doświadczenie, tj. dyplomy, certyfikaty czy przebieg dotychczasowego zatrudnienia. Wskazówki Biura GIODO pomocne w dokonywaniu oceny kwalifikacji zatrudnianej na to stanowisko osoby zamieściliśmy w dostępnym na naszej stronie internetowej serwisie ABI-Informator w zakładce „Pytania i odpowiedzi” w sekcji „Inspektor ochrony danych”.

W przypadku placówek z sektora medycznego, które przetwarzają przecież dane wrażliwe, trzeba szczególnie starannie sprawdzać tę wiedzę i wymagać poziomu zaawansowanego.

W przypadku ABI pracujących dla szpitali i przychodni nie chodzi tylko o wiedzę i doświadczenie z zakresu stosowania przepisów zawartych w ustawie czy rozporządzeniu o ochronie danych osobowych, ale też o znajomość bardzo wielu przepisów branżowych dotyczących przetwarzania danych pacjentów, na przykład ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, ustawy o systemie informacji w ochronie zdrowia, ustawy o zawodzie pielęgniarki i położnej i wielu innych. Ważna jest też znajomość funkcjonowania danej organizacji, podziału zadań i kompetencji, schematu organizacyjnego, przepływu danych pomiędzy poszczególnymi komórkami organizacyjnymi.

Ponieważ do zadań takiej osoby należy nadzór nad ochroną danych osobowych, to jej wiedza musi obejmować znajomość wszystkich szczegółów dotyczących danych osobowych, tzn. na przykład tego, jakie dane, w jaki sposób, w jakim celu, przez kogo i konkretnie gdzie są w dalej placówce przetwarzane, jakie osoby mają do nich dostęp oraz jakie zagrożenia dla bezpieczeństwa tych danych zostały dotychczas zidentyfikowane.

Jakie zadania nakłada na inspektorów rozporządzenie unijne?

Do zadań inspektora będzie należało doradzanie i informowanie w zakresie obowiązków, jakie na osoby przetwarzające dane i podejmujące decyzje nakładają przepisy prawa. Inspektor ma też nadzorować, czy obowiązki te są prawidłowo wykonywane, na przykład za pomocą sprawdzeń, audytów zgodności przetwarzania danych z przepisami RODO i wewnętrznymi regulacjami podmiotu, tzw. wewnętrznymi politykami.

Istotnym polem dla działań doradczych i weryfikacyjnych inspektorów ochrony danych będzie tzw. ocena skutków dla ochrony danych. To nowy obowiązek przewidziany przez rozporządzenie ogólne, który polega na szczegółowym badaniu tych operacji przetwarzania, które z „dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych”. Przykładem przetwarzania wymagającego takiej oceny jest przetwarzanie na dużą skalę danych osobowych o stanie zdrowia.

Inspektor ochrony danych osobowych będzie miał także obowiązek współpracowania z organem nadzorczym, czyli z GODO. W przepisach określono, że inspektor ma pełnić rolę punktu kontaktowego dla organu nadzorczego w każdym przypadku, gdy zajdzie taka potrzeba.

Obowiązkiem inspektora będzie również udzielanie pomocy osobom, których dane placówka przetwarza, tzn. objaśnianie im ich uprawnień i ułatwianie korzystania z nich, na przykład z uprawnienia do dostępu do danych. Przepis rozporządzenia ogólnego stanowi, że każda osoba może kontaktować się z inspektorem ochrony danych we wszelkich sprawach, które dotyczą przetwarzania jej danych osobowych. Inspektor ochrony danych będzie więc swego rodzaju „tarczą” administratora danych, fachowym łącznikiem między nim a osobami, którym placówka świadczy usługi medyczne.

Jednak trzeba podkreślić, że odpowiedzialność za przetwarzanie danych osobowych zgodnie z prawem cały czas będzie spoczywała na administratorze tych danych. Zatrudnienie inspektora nie zdejmuje z administratora tej odpowiedzialności. Inspektor będzie wprowadzać przekazywał swoje uwagi, wytyczne czy wskazówki, ale to administrator, osoba zarządzająca będzie odpowiedzialna za ich wprowadzenie w życie.

Zadania inspektora to nie tylko nadzór nad ochroną danych....

Do istotnych zadań inspektora będą należały także wewnętrzne działania edukacyjno-szkoleniowe. Jeśli osoby kierujące placówką i jej pracownicy znają zasady i wymogi prawne oraz rozumieją, czemu one mają służyć, zwykle starają się ich przestrzegać. Stąd rola inspektora w tym zakresie jest nie do przecenienia.

Ponadto inspektor to osoba, która ma uświadamiać zagrożenia, ryzyka, związane z przetwarzaniem danych oraz konsekwencje związane z nieprzestrzeganiem przepisów. A te w RODO są dużo poważniejsze niż dotychczas.

Dlatego świadomość dotycząca ochrony danych osobowych jest bardzo ważna. Dane osobowe w placówce medycznej muszą być chronione na każdym etapie - od recepcji przez laboratoria, aż do lekarzy i ordynatorów oddziałów szpitalnych oraz dyrektorów szpitali.

Doświadczeni ABI zatrudnieni w szpitalach prowadzą działania szkoleniowo-edukacyjne w ten sposób, że dzielą personel na medyczny i niemedyczny, dostosowując przekazywane treści do potrzeb i obowiązków określonych grup.

Warto też zaznaczyć, że coraz więcej jest pacjentów, którzy mają świadomość obowiązujących przepisów, domagają się odpowiedniego traktowania, co też wymusza na placówkach medycznych odpowiednie rozwiązania.

Coraz bardziej przebija się to także do świadomości lekarzy, którzy wiedzą, że na przykład rozmowy dotyczące spraw objętych tajemnicą medyczną nie mogą być prowadzone przy innych pacjentach.

Jednak ABI sygnalizują nam, że w sektorze medycznym czasem trudno im się przebić ze swoimi radami, gdyż jego pracownicy są tak bardzo skupieni są na swojej głównej misji, którą jest ratowanie zdrowia i życia, że nie mają już możliwości i czasu, żeby poświęcać go innym zagadnieniom. Ponadto w obszarze medycznym jest tak duża liczba niezaspokojonych potrzeb, zarówno finansowych, kadrowych, jak i organizacyjnych, że gdy wspomina się jeszcze o dodatkowych obowiązkach związanych z ochroną danych osobowych, za którymi nie idą dodatkowe pieniądze, to często budzi to opór. Widoczne jest to szczególnie w placówkach publicznych. Prywatne, które są zasobniejsze i działają na konkurencyjnym rynku, dbając o swój wizerunek, nie chcą dopuszczać do jakichkolwiek nieprawidłowości, w tym także w zakresie ochrony danych osobowych.

Niemniej przestrzeganie przepisów o ochronie danych osobowych jest obowiązkiem, z którego muszą rozliczyć się wszystkie podmioty, i publiczne, i prywatne w państwach członkowskich Unii Europejskiej.

Na jakich zasadach powinien być w placówce medycznej zatrudniony inspektor ochrony danych? Czy to musi być pracownik etatowy?

RODO wyraźnie wskazuje, że inspektor ochrony danych osobowych nie musi być pracownikiem zatrudnionym na etat. Może to być także osoba, z którą podpisana zostanie

umowa cywilno-prawna. Przepisy stanowią także, że jeden inspektor może obsługiwać kilka podmiotów. Dotyczy to na przykład przedsiębiorstw należących do jednej grupy kapitałowej. Ale z rozwiązania tego mogą też korzystać podmioty publiczne.

Przy czym wspomnieć należy o występujących dodatkowych wymogach. W przypadku grupy przedsiębiorstw wymóg dotyczy tego, że inspektor ma być łatwo dostępny dla każdej jednostki organizacyjnej należącej do grupy. Grupa Robocza Art. 29 rozwija go, wskazując, że taka osoba musi być dostępna nie tylko dla przedstawicieli poszczególnych organizacji, ale też dla podmiotów, których dane są przetwarzane przez te placówki, a także dla organów nadzorczych.

W przypadku podmiotów publicznych trzeba uwzględnić ich strukturę organizacyjną i wielkość. Zarządzający tymi placówkami powinni więc ocenić, czy jeden inspektor będzie miał możliwość rzetelnego i prawidłowego obsługiwanie wszystkich podmiotów, które będzie miał pod opieką.

W przypadku mniejszych podmiotów, na przykład niewielkich poradni specjalistycznych, w których pracuje dwóch czy trzech lekarzy, zatrudnienie jednego inspektora, obsługującego kilka takich podmiotów może okazać się dobrym, racjonalnym pomysłem. Ale trudno sobie wyobrazić takie rozwiązanie w przypadku dużych klinicznych szpitali.

Z pewnością sytuacje wyznaczania jednej osoby przez zbyt wielu administratorów danych zweryfikuje praktyka, zadziała tu wspomniana zasada rozliczalności i większej odpowiedzialności administratorów danych. Chodzi o to, aby inspektor ochrony danych, niezależnie, na jakich zasadach został zatrudniony, był dostępny zawsze, gdy jest potrzebny i aby mógł zareagować w sytuacji zagrożenia lub naruszenia. Nowe przepisy wymagają bowiem szybkiego, efektywnego działania na przykład w przypadku wykrycia naruszenia ochrony danych osobowych. Przepisy określają między innymi, że placówki mają 72 godziny na to, aby zgłosić naruszenie ochrony danych osobowych. Jest to obowiązek administratora, ale w zawiadomieniu tym należy podać imię i nazwisko inspektora, od którego można uzyskać więcej informacji o tym, co się wydarzyło, w jaki sposób placówka zamierza zapobiec skutkom tego zdarzenia, czy należy zawiadomić osobę lub osoby, których dane zostały naruszone.

ABI zgłaszają nam obecnie, że w modelu „jeden dla kilku” może wystąpić wiele, trudnych do pokonania problemów, na przykład dużo łatwiej o konflikt interesów. Ponadto warto zaznaczyć, że aby zapewnić obsługę każdemu z podmiotów w sposób odpowiedzialny i rzetelny, trzeba zaangażować wiele czasu i wysiłku, świetnie znać wszystkie aspekty funkcjonowania danej placówki mające znaczenie dla jej zgodnego z prawem działania. Jeżeli zatem ktoś podchodzi do kwestii bezpieczeństwa danych osobowych odpowiedzialnie, będzie z pewnością szukał własnego, dyspozycyjnego i zaangażowanego w pełnienie swojej funkcji inspektora. Dlatego uważam, że wejście do stosowania RODO przyniesie kres zdarzającym się obecnie sytuacjom, że jeden inspektor obsługuje kilkadziesiąt lub nawet sto kilkadziesiąt podmiotów.

Jak powinien być usytuowany pod względem organizacyjnym inspektor ochrony danych w placówce medycznej?

Najlepszym rozwiązaniem dla zachowania niezależności inspektora jest samodzielne

stanowisko. Zarówno z ustawy o ochronie danych osobowych, jak i z przepisów rozporządzenia wynika, że powinna to być osoba, która bezpośrednio podlega najwyższemu kierownictwu, czyli kierownikowi jednostki organizacyjnej.

Ma to na celu skrócenie drogi raportowania, ma też ułatwiać kontrolę procedur przetwarzania danych. Jest to jedna z ważnych gwarancji niezależności inspektora.

Taką funkcję mogą pełnić na przykład dyrektorzy departamentów zajmujący się zapewnianiem zgodności działania z prawem (np. działy compliance, niestety rzadko występujące w placówkach medycznych). Ale trzeba też pamiętać, że tej funkcji nie można łączyć z takimi stanowiskami kierowniczymi, na których podejmuje się decyzje dotyczące celów i środków przetwarzania. Jest tak dlatego, że w takiej sytuacji występuje konflikt interesów wynikający z tego, że ta sama osoba nie może decydować o sposobie przetwarzania i zabezpieczania danych osobowych, a jednocześnie weryfikować tych decyzji pod kątem ich zgodności z prawem. Dlatego Grupa Robocza Art. 29 podkreśla, że ten konflikt interesów występuje w przypadku większości stanowisk kierowniczych.

Niezależność to chyba najważniejsza cecha inspektora...

Zgadza się, dlatego w rozporządzeniu znalazł się między innymi przepis, że inspektora nie można karać ani zwolnić za wykonywanie należących do niego zadań. Czyli w sytuacji, gdy inspektor wykonuje swoją funkcję prawidłowo, z dużym zaangażowaniem, aktywnie i asertywnie wskazuje kierownictwu placówki, co należy zmienić, żeby przeciwdziałać nieprawidłowościom, a kierownictwo tej placówki odbiera te działania jako kłopotliwe, niewygodne i chce z tego powodu zwolnić inspektora, to taki inspektor ma wówczas zapewnioną ochronę i szansę na wygranie sprawy w sądzie pracy. Działal przecież w najlepiej pojmowanym interesie administratora danych i zgodnie z prawem.

Administrator powinien okazywać wsparcie inspektorowi ochrony danych osobowych, zapewniać mu odpowiednie zasoby, środki niezbędne do prawidłowego wykonywania funkcji. Do takich zasobów zalicza się także środki finansowe przeznaczone na podnoszenie kwalifikacji. Wymóg uaktualniania wiedzy i zapewnienia na to środków finansowych jest zupełnie uzasadniony wobec ciągle zmieniającego się stanu wiedzy technicznej, rozwoju technologicznego i postępu w zakresie metod przetwarzania i zabezpieczania danych. Można z pewnością powiedzieć, że w tę funkcję wpisane jest ciągle kształcenie, uwzględnianie zmian w prawie i praktykach związanych ze skuteczną ochroną danych osobowych. Praktyki administratorów danych muszą być dostosowywane do zmieniających się ryzyk i zagrożeń.

Ile placówek medycznych zatrudnia obecnie administratorów bezpieczeństwa informacji?

Gdy w marcu 2017 roku organizowaliśmy szkolenie dla ABI z sektora medycznego, okazało się, że jest to sektor, w którym bardzo wiele podmiotów powołało swoich ABI. Na organizowane przez GIODO szkolenie zgłosiło się ponad 400 osób! Dlatego wszystkich chętnych musieliśmy podzielić na dwie grupy i zorganizować dwa szkolenia. Oczywiście nie byli to administratorzy bezpieczeństwa informacji ze wszystkich placówek medycznych, a i tak z momentem wejścia do stosowania RODO, liczba ABI – przyszłych inspektorów ochrony danych w tym sektorze ulegnie bardzo dużemu zwiększeniu. Placówki, które

wcześniej zatrudniły taką osobę i już obecnie korzystają z jej pomocy, na pewno są w lepszej sytuacji niż te, które będą dopiero jej szukać.

W jakim terminie szpital musi zgłosić fakt zatrudnienia inspektora ochrony danych do GODO?

Obecne przepisy stanowią, że od momentu powołania administratora bezpieczeństwa informacji placówka ma 30 dni na zgłoszenie tego faktu do GODO.

Po 25 maja 2018 roku podmioty, które będą miały obowiązek wyznaczania inspektora ochrony danych, lub zdecydują się na wyznaczenie takiej osoby, mimo że obowiązek nie będzie ich dotyczył, będą musiały powiadomić organ nadzorczy o tzw. danych kontaktowych takiej osoby, oraz udostępnić te dane wszystkim zainteresowanym osobom, na przykład na swojej stronie internetowej. Przepisy przejściowe, które przygotowujemy są obecnie w Polsce, będą doprecyzowały sposób dopełniania tego obowiązku i tego, w jakim terminie należy go dopełnić i jaki dokładnie dane podać. Warto pamiętać, że obowiązek taki będzie dotyczył każdego administratora czy podmiotu przetwarzającego, który wyznaczy inspektora, nawet w modelu „jeden inspektor dla kilku podmiotów”.

Jakie sankcje będą groziły placówkom za niezatrudnienie inspektora ochrony danych?

Jeżeli placówka nie wyznaczy inspektora ochrony danych, mimo istnienia takiego obowiązku, GODO będzie uprawniony do podjęcia działań naprawczych, włącznie z zastosowaniem administracyjnej kary pieniężnej określonej w art. 83 rozporządzenia ogólnego.

Myślę jednak, że o zgodność z przepisami rozporządzenia ogólnego warto zadbać odpowiednio wcześniej nie z powodu kar, ale dlatego, że te nowe zasady są dużą szansą na zrewidowanie i ulepszenie dotychczasowych procedur i praktyk w zakresie ochrony danych osobowych, tak by przynosiły one korzyści i placówce medycznej, i jej pacjentom. Żeby pomóc w tym administratorom danych, w pierwszym okresie stosowania rozporządzenia (tak zresztą, jak obecnie) będziemy prowadzić wiele działań informacyjnych, edukacyjnych i szkoleniowych. Wiele pomocnych informacji dotyczących inspektorów ochrony danych można znaleźć np. we wspomnianym serwisie – ABI Informator, gdzie między innymi odpowiadamy na pytania przekazywane przez zainteresowane osoby. Współtwórcami tych informacji są zatem administratorzy bezpieczeństwa informacji, którzy przekazują nam swoje wątpliwości i podpowiadają zagadnienia, jakie w tym serwisie powinniśmy poruszyć.

Rozmawiała: Magdalena Okoniewska