Warszawa, dnia 30 czerwca 2017 roku

Stanowisko Izby Gospodarki Elektronicznej
w ramach konsultacji projektu dokumentu pn.
„Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej."

Izba Gospodarki Elektronicznej jako rzecznik przedsiębiorców z branży e-zdrowie pragnie ustosunkować się do *projektu dokumentu* przedstawionego przez *Centrum Systemów Informacyjnych Ochrony Zdrowia pn.* **„Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej." (dalej: Rekomendacje lub Dokument).**

Na wstępie chcielibyśmy zaznaczyć, że zarówno fakt stworzenia Rekomendacji, jak i otwartość *Centrum Systemów Informacyjnych Ochrony Zdrowia* (dalej: CSIOZ) na uwagi i opinie środowisk związanych z ochroną zdrowia i IT **z pewnością stanowią** doskonały punkt wyjścia do podjęcia dyskusji na temat zasad przetwarzania danych medycznych. **Generalnie Dokument jest potrzebny i zawiera wartościowe dla placówek medycznych informacje i wskazówki**, które z pewnością będą przydatne dla świadczeniodawców stojących przed wyzwaniem cyfryzacji dokumentacji medycznej. Dostrzegamy, iż ranga Dokumentu wykracza dalece ponad potoczne znaczenie pojęcia „rekomendacje", co również uważamy za właściwe.

Poniżej pragniemy zwrócić uwagę jedynie na wybrane aspekty, które w naszej ocenie można i należy poprawić.

1) Uwagi ogólne

Rekomendacje przeznaczone są dla świadczeniodawców, którzy przetwarzają już dokumentację medyczną w formie cyfrowej, jak również dla podmiotów z branży medycznej, które dopiero przygotowują się lub też wdrażają w swoich placówkach systemy informatyczne służące do przetwarzania dokumentacji medycznej. Z tego względu, Dokument powinien być czytelny zarówno dla przedstawicieli placówek medycznych, którzy posiadają już pewną wiedzę w temacie rozwiązań służących wdrożeniu elektronicznej dokumentacji medycznej (dalej: EDM), jak i reprezentantów placówek medycznych, które dopiero zamierzają wprowadzić niezbędne rozwiązania techniczne do prowadzenia dokumentacji medycznej w postaci cyfrowej. Wskazać należy, że język, niedostateczne wyjaśnienie pewnych terminów i instytucji prawnych, jak i sformułowań i terminologii o charakterze techniczno-informatycznym sprawiają, że Rekomendacje w aktualnym brzmieniu są trudne w odbiorze, przez co główny przekaz Rekomendacji jest mało czytelny.

T + 48 500 390 172 E BIURO@EIZBA.PL I WWW.E-IZBA.PL
A PAŃSKA 96,LOK 83, 00-837 WARSZAWA NIP 701-039—19-22 KRS 0000474028

W ocenie Izby Gospodarki Elektronicznej Rekomendacje powinny w wyraźny i czytelny sposób odróżniać i precyzować, które rozwiązania techniczne i prawne są wymogiem nałożonym przez obowiązujące przepisy prawa, a które stanowią zalecane przez CSIOZ wymagania oraz możliwe i pożądane sposoby ich realizacji. Takie rozróżnienie z pewnością ułatwi adresatom Dokumentu jego zrozumienie, a tym samym pozwoli im lepiej przygotować się do wdrożenia EDM.

2) Obowiązujące przepisy prawa dotyczące ochrony danych osobowych oraz przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Problematykę ochrony danych osobowych aktualnie reguluje ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz wydane na jej podstawie rozporządzenia wykonawcze. Sektorowe akty prawne w dziedzinie ochrony zdrowia w zakresie przepisów odnoszących się do dokumentacji medycznej również szczątkowo normują tę kwestię.

Co istotne, przepisy ustawy o ochronie danych osobowych stanowią realizację wymagań zawartych w Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Tymczasem, już 25 maja 2018 roku stosowane będzie Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (dalej: RODO), które wprowadza istotne zamiany dotyczące przetwarzania i ochrony danych osobowych (a w tym danych medycznych) w stosunku do aktualnie obowiązujących aktów prawnych.

Odbiorca Rekomendacji powinien mieć pełną świadomość, że znacząca część przedstawionych w Dokumencie zaleceń stanie się nieaktualna w momencie rozpoczęcia obowiązywania przepisów RODO. W tym celu należy wyraźnie wskazywać, które obowiązki skończą się z dniem 25 maja 2018 r., które będą zupełnie nowe, a które ulegną modyfikacji.

Mając na uwadze fakt, iż wprowadzone rozwiązania informatyczne i proceduralne dotyczące przetwarzania dokumentacji medycznej w formie elektronicznej winny być jak najdłużej aktualne pod względem technologicznym i prawnym, proponowane przez CSIOZ Rekomendacje powinny uwzględniać odpowiednią perspektywę czasową. Tym samym, powinny zawierać m.in. ocenę regulacji prawnych, które już weszły w życie, ale dopiero zaczną obowiązywać. Tak jest w przypadku **RODO, którego przepisy** mają być stosowane od dnia 25 maja 2018 r. Stosunkowo bliski termin oznacza, że podmiot planujący wdrożenie systemu informatycznego służącego do przetwarzania EDM powinien uwzględnić także normy, które dopiero zaczną obowiązywać. W przeciwnym wypadku zaprojektowany i

wdrożony system informatyczny oraz wprowadzone rozwiązania i procedury w zakresie bezpieczeństwa danych medycznych w krótkim czasie stanie się niedostosowane do nowych uwarunkowań prawnych. Z tych względów Izba Gospodarki Elektronicznej rekomenduje, aby Rekomendacje w swoich założeniach były zgodne ze stanem prawnym w zakresie ochrony danych osobowych na dzień 25 maja 2018 roku.

3) Uwagi szczegółowe dotyczące wskazanych w Rekomendacjach wymogów prawnych oraz proponowanych rozwiązań z zakresu ochrony danych osobowych

a) Konieczność wskazania lokalizacji, w której przetwarzane są dane, a ograniczenia dotyczące wykorzystania do przetwarzania danych medycznych rozwiązań bazujących na chmurze obliczeniowej

W Rekomendacjach wskazano, że z uwagi na ograniczenia wynikające z przepisów prawa usługodawca nie ma możliwości wykorzystania do przetwarzania danych medycznych rozwiązań bazujących na chmurze obliczeniowej (rozdział 2, pkt. 2.3. Cloud computing (chmura obliczeniowa). Autorzy Rekomendacji podnoszą, że „w przypadku zlecenia przetwarzania i archiwizowania dokumentacji medycznej w postaci elektronicznej wymagana jest jednoznaczna identyfikacja miejsca przetwarzania danych medycznych. Oznacza to, że usługodawca powinien posiadać wiedzę, w którym systemie (aplikacja, baza danych, itp.) oraz na którym urządzeniu fizycznym (serwer, dysk, macierz dyskowa, taśma do backupu, itp.) będą przetwarzane, przechowywane i archiwizowane jego dane medyczne”, w związku z czym w przypadku wykorzystania chmury obliczeniowej „usługodawca ma obowiązek posiadania wiedzy, na którym serwerze będą archiwizowane jego dane medyczne”.

Powyższe stwierdzenia są w ocenie Izby Gospodarki Elektronicznej aktualne na gruncie obowiązujących przepisów. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 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 przewiduje bowiem obowiązek wskazania w dokumencie „Polityka bezpieczeństwa” obowiązek wskazania „wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe”. Do posiadania i wdrożenia Polityki bezpieczeństwa obligują administratora danych, jakim niewątpliwie będzie każda placówka medyczna, zarówno przepisy ustawy o ochronie danych osobowych, jak i przepisy ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Podkreślić jednak należy, że RODO w zupełnie odmienny sposób reguluje obowiązki dokumentacyjne administratora danych, a także zasady zabezpieczenia danych osobowych. RODO wprowadza istotną zmianę podejścia do zabezpieczania danych osobowych. Nie opisuje konkretnych mechanizmów bezpieczeństwa w warstwie technologicznej, proceduralno-procesowej i organizacyjnej, które muszą być wdrożone, a jedynie ogólne wymagania w obszarze bezpieczeństwa danych osobowych. W związku z tym, sposób spełnienia tych wymagań dla różnych

podmiotów może być inny, a nawet dla jednego podmiotu może istnieć kilka scenariuszy.

Art. 32 ust. 1 RODO wskazuje, że administrator i podmiot przetwarzający uwzględniając 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, wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Oznacza to, że placówki medyczne jako administratorzy danych, a także w pewnych wypadkach podmioty przetwarzające dane na zlecenie, samodzielnie będą decydować jakie środki będą adekwatne celem zabezpieczenia przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Nadto, RODO nie nakłada na administratora danych, czy podmiot przetwarzający obowiązku podania dokładnej lokalizacji przetwarzanych danych.

W konsekwencji, zaprezentowane w Rekomendacjach twierdzenia, jakoby konieczna była jednoznaczna identyfikacja miejsca przetwarzania danych medycznych będą wkrótce nieaktualne. Możliwe i zgodne z przepisami prawa będzie zaś przetwarzanie danych medycznych przy użyciu rozwiązań bazujących na chmurze obliczeniowej. Podkreślić przy tym należy, że mając na uwadze tak szybki rozwój nowych technologii oraz dostępnych sposobów zabezpieczeń danych wprowadzone przez ustawodawcę europejskiego rozwiązanie zasługuje na aprobatę.

b) Inspektor ochrony danych

W Rekomendacjach (rozdział 4, pkt 4.1.1. Wymagania personalne z zakresu ochrony danych osobowych w tym danych medycznych) zwrócono uwagę na możliwość powołania przez usługodawców administratora bezpieczeństwa informacji (ABI), opisano podstawowe zadania osoby pełniącej tę funkcję oraz wskazano na konsekwencje powołania ABI. W Rekomendacjach zabrakło jednak podobnej analizy funkcji inspektora ochrony danych, którego wyznaczenie będzie obligatoryjne dla wszystkich usługodawców po 25 maja 2018 r.

Zgodnie z art. 37 ust. 1 RODO administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy: przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości lub w sytuacji, gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, do których zaliczają się dane medyczne. W pozostałych przypadkach wyznaczenie inspektora ochrony danych jest fakultatywne.

Inspektor ochrony danych będzie miał obowiązki zbliżone do ABI, jednakże RODO nakłada na podmiot pełniący tę funkcję także inne, dodatkowe obowiązki np. **udzielanie na żądanie administratora zaleceń** co do oceny skutków dla ochrony

danych oraz monitorowanie jej wykonania, czy też pełnienie funkcji **punktu kontaktowego** dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych. W ocenie Izby Gospodarki Elektronicznej rekomendacje winny dokładnie precyzować zakres obowiązków inspektora danych osobowych.

Podkreślenia wymaga przy tym, że RODO nakłada na administratorów oraz podmioty przetwarzające dane na ich zlecenie obowiązek publikacji danych inspektora oraz powiadomienia o nich organów nadzorczych, jako jeden z elementów spełnienia obowiązku informacyjnego. W Rekomendacjach nie zawarto informacji w tym przedmiocie.

c) Obowiązki rejestracyjne administratorów danych

W rozdziale 4 w pkt. 4.1.2. Rekomendacji szczegółowo opisano obowiązki rejestracyjne administratorów danych. Tymczasem RODO znosi obowiązek zgłaszania zbiorów danych osobowych do GIODO. Zamiast tego nakazuje jednak prowadzenie wewnętrznego rejestru przetwarzania. Zawartość rejestru będzie zbliżona do treści obecnie dokonywanych zgłoszeń (będzie zawierał m.in. kategorie danych osobowych, kategorie osób, których dane dotyczą, cele przetwarzania i kategorie odbiorców). Rejestr będą jednak musieli prowadzić nie tylko administratorzy, ale także podmioty przetwarzające dane na zlecenie administratora (np. dostawca hostingu, firma oferująca outsourcing księgowy).

Formalnie z obowiązku prowadzenia rejestru zwolnione będą podmioty zatrudniające mniej niż 250 osób. Wyłączenie to nie ma jednak zastosowania, gdy przetwarzanie „może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą" (np. ryzyko ujawnienia danych osobom niepowołanym), „nie ma charakteru sporadycznego" (a więc następuje regularnie, choćby w niewielkiej skali) lub dotyczy danych wrażliwych, do których należą dane medyczne. Rejestry przetwarzania będą zatem musiały prowadzić wszystkie placówki medyczne, o czym w ogóle nie wspomniano w Rekomendacjach.

d) Inne obowiązki dokumentacyjne administratora danych

Obok wskazanego wyżej rejestru przetwarzania, administrator danych będzie miał inne obowiązki dokumentacyjne, których nie wskazano w Rekomendacjach.

Każdy administrator będzie zobowiązany dokumentować „wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze". Definicja „naruszenia ochrony danych" może przy tym obejmować nie tylko przypadki włamań do systemów informatycznych, ale także zgubienie laptopa czy wysłanie e-maila do niewłaściwej osoby.

RODO zobowiązuje też administratorów danych do przeprowadzenia tzw. oceny skutków przetwarzania wtedy, gdy przetwarzanie „z dużym prawdopodobieństwem

może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych". RODO precyzuje, że ma to miejsce w szczególności w przypadku a) systematycznego i kompleksowego zautomatyzowanego przetwarzania prowadzącego do podejmowania wobec jednostek istotnych dla nich decyzji b) przetwarzania danych wrażliwych „na dużą skalę" i c) „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie". Obowiązkowa ocena skutków przetwarzania będzie z pewnością dotyczyć podmiotów z sektora usług medycznych.

Ocena skutków przetwarzania służy szacowaniu ryzyka naruszenia praw lub wolności osób, których dane dotyczą (np. ryzyka nieuprawnionego ujawnienia danych, ryzyka podjęcia błędnych decyzji), a także ustaleniu środków ograniczenia tego ryzyka. Ocena skutków przetwarzania musi obejmować systematyczny opis planowanych operacji przetwarzania i celów przetwarzania oraz ustalenie, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów (tj. np. czy zamierzone cele można by osiągnąć, zbierając mniej danych). Przedsiębiorcy „narażeni" na dokonywanie oceny skutków przetwarzania powinni rozważyć stworzenie wewnętrznych wytycznych i formularzy wspomagających ten proces (wskazujących kiedy należy go wdrożyć i co należy zweryfikować).

Przygotowany przez CSIOZ Dokument regulując zasady przetwarzania danych osobowych powinien w pełni opisywać obowiązki nałożone na placówki medyczne pełniące funkcję administratorów danych medycznych. Konieczne jest zatem uzupełnienie Dokumentu o szczegółowy opis wszystkich obowiązków nałożonych na administratorów danych i podmioty przetwarzające dane na ich zlecenie przepisami RODO.

e) Umowa powierzenia przetwarzania danych osobowych

Rekomendacje w rozdziale 4, w pkt. 4.2 – Minimalne wymagania dotyczące bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej wskazują elementy jakie powinna zawierać umowa powierzenia przetwarzania danych. Instytucja powierzenia przetwarzania danych z pewnością będzie często wykorzystywana przez placówki medyczne w związku z wdrożeniem dokumentacji medycznej w formie cyfrowej. Istotne jest zatem, aby podmioty, do których skierowane są Rekomendacje posiadały pełną informację na temat umowy powierzenia.

RODO w sposób zdecydowanie bardziej szczegółowy reguluje omawianą instytucję, niż ma to miejsce na gruncie ustawy o ochronie danych osobowych. W rozporządzeniu unijnym wskazano na konieczność zawarcia w umowie powierzenia wielu dodatkowych elementów. Ponadto, administrator w umowie tej powinien nałożyć na podmiot przetwarzający liczne obowiązki, których spełnienie nie było dotychczas wymagane. Najistotniejsza zmiana w tym przedmiocie dotyczy jednak do obowiązku administratora korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Niespełnienie powyższego obowiązku stanowić będzie

naruszenie przepisów rozporządzenia unijnego przed administratora, co zagrożone będzie surowymi karami pienionymi. W praktyce obowiązek ten oznaczać będzie konieczność prowadzenia audytów u podmiotów, którym administrator będzie chciał powierzyć przetwarzanie danych (np. podmiotów świadczącym usługi w zakresie hostingu danych). Rekomendacje powinny zawierać szczegółowe wytyczne i zalecenia w tym zakresie.

f) Bezpieczeństwo systemów informatycznych i dokumentacji medycznej

Rekomendacje w rozdziale 4 w pkt 4.2.2 zawierają opis środków technicznych i organizacyjnych jakie muszą zostać wdrożone przez administratora danych będącego placówką medyczną odnosząc się do wymagań zawartych w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Tymczasem, jak już wskazano wyżej RODO wprowadza odmienne podejście do zabezpieczania danych osobowych. Rozporządzenie unijne nie opisuje konkretnych mechanizmów bezpieczeństwa w warstwie technologicznej, proceduralno-procesowej i organizacyjnej, które muszą być wdrożone, a jedynie ogólne wymagania w obszarze bezpieczeństwa danych osobowych.

Rekomendacje stwarzają wrażenie, że wystarczające jest wdrożenie przez placówki ściśle określonych środków (zwartych w ww. rozporządzeniu Ministra Spraw Wewnętrznych i Administracji) dla zapewnienia bezpieczeństwa przetwarzania danych osobowych, w tym danych medycznych, wymaganego przepisami prawa. Tymczasem, z uwagi na szybki i nieustający rozwój technologii metody zabezpieczani wymienione w rozporządzeniu, które zostało wydane w 2004 r. mogą okazać się niewystarczające. Nowe rozwiązania IT pozwalają lepiej chronić dane osobowe, a jednocześnie stwarzają coraz większe zagrożenie nieuprawnionego dostępu, czy ataku hackerskiego. Rozwiązania przewidziane w RODO wymagają od administratorów danych oraz podmiotów przetwarzających dane osobowe na ich zlecenie ciągłego udoskonalania stosowanych metod służących do zabezpieczenia danych, czego usługodawcy powinni mieć świadomość.

g) Zmiany w zakresie uzyskiwania zgody na przetwarzanie danych osobowych

Izba Gospodarki Elektronicznej zwraca również uwagę na fakt, iż RODO wprowadza istotne zmiany w zakresie zgody na przetwarzanie danych osobowych. Odbiorcy Rekomendacji powinni mieć świadomość, że w pewnych wypadkach niezbędne będzie uzyskanie zgody na przetwarzanie danych osobowych pacjentów, w tym przetwarzanie ich danych wrażliwych, oraz jakie są warunki uzyskania takiej zgody.

Zasadniczą zmianą, którą w praktyce odczują wszystkie podmioty przetwarzające dane osobowe, będzie konieczność dostosowania procedur pozyskiwania zgody na przetwarzanie danych osobowych do nowych przepisów. Prawidłowe przygotowanie procesu pozyskiwania zgody, czy też formularzy zgody, to zadanie, do którego

placówki medyczne powinny się przygotować, gdyż konsekwencje naruszenia przepisów w tym zakresie mogą być bardzo dotkliwe. Po pierwsze, gdy zgoda zostanie uzyskana nieprawidłowo będzie nieważna – a zatem podmiot, który ją pozyskał nie będzie mógł na jej podstawie danych osobowych przetwarzać. Po drugie, zgodnie z nowymi regulacjami, za naruszenie przepisów dotyczących zgody będzie nakładana przez GIODO kara administracyjna w wysokości do 20 mln euro lub w wysokości do 4 proc. całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego

Katalog sytuacji, w których możliwe jest przetwarzanie danych osobowych, zasadniczo nie ulegnie zmianie. Jedną z przesłanek dopuszczalności przetwarzania będzie nadal uzyskanie zgody osoby, której dane dotyczą. RODO doprecyzowuje jednak, jakie warunki powinna spełniać zgoda. Musi to być dobrowolne, konkretne, świadome i jednoznaczne okazanie woli. Ponadto, zgoda musi mieć charakter wyraźnego działania – oświadczenia lub potwierdzenia. W praktyce oznacza to, że formularze zgody powinny być sformułowane jasnym i czytelnym językiem, tj. w sposób zrozumiały dla osoby, której dane dotyczą.

Co istotne, w wypadku danych wrażliwych, czyli m.in. danych medycznych nie będzie już wymagana zgoda na piśmie – wystarczające będzie uzyskanie zgody „wyraźnej". Jednakże, **administrator danych będzie musiał być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę** na przetwarzanie jej danych osobowych. Izba Gospodarki Elektronicznej stoi na stanowisku, że informacje w tym przedmiocie powinny zostać umieszczone w Rekomendacjach.

h) Brak wytycznych i zaleceń w jaki sposób placówki zdrowotne mają przygotować się do nowych obowiązków wynikających z RODO

Zważywszy na bliski termin obowiązku stosowania się do wymogów RODO, Rekomendacje powinny w sposób kompleksowy opisywać w jaki sposób placówki medyczne powinny przygotować się do obowiązków nałożonych na nie przez rozporządzenie unijne.

Mając na względzie rozległość procesów przetwarzania prowadzonych przez usługobiorców z sektora medycznego, istotne jest rozpoczęcie planowania podejścia w zakresie zgodności z RODO tak wcześnie jak to możliwe. Przedstawiciele tych podmiotów powinni zostać poinformowani od czego zacząć przygotowania, w jaki sposób je przeprowadzić, jakie dokumenty należy stworzyć i w jaki sposób dokonać oceny poziomu bezpieczeństwa, który musi zostać zagwarantowany przez placówkę medyczną. Rekomendacje powinny również pomóc w opracowaniu działań wdrożeniowych i naprawczych, w tym zaplanowaniu ciągłego procesu weryfikacji i uwzględniania ochrony danych osobowych.

Rekomendacje nie zawierają żadnych wytycznych w tym zakresie, co niewątpliwie wymaga uzupełnienia.

4) Zalecenie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji

Rekomendacje, w rozdziale 6, w celu zapewnienia bezpieczeństwa dokumentacji medycznej, zalecają wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z wymaganiami normy ISO/IEC 27001 (dalej: SZBI)**, którego plan wdrożenia został ujęty w rozdziale 7 Dokumentu.**

Wskazać należy, że na gruncie aktualnie obowiązujących przepisów wdrożenie powyższego systemu przez administratorów danych osobowych jest dobrowolne. Jego funkcjonowanie zasadza się na – konkretnym, zamkniętym – zbiorze reguł i procedur. Umożliwiają one ustanowienie, wdrożenie, monitorowanie, przegląd, utrzymanie i doskonalenie polityki bezpieczeństwa organizacji.

Zwracam jednak uwagę, że RODO wprowadza dwa rozwiązania prawne: kodeksy postępowania oraz certyfikację wraz z oznaczeniami i znakami jakości ochrony danych osobowych, których celem jest po pierwsze pomoc administratorom danych osobowych we właściwym stosowaniu RODO, a po drugie zapewnienie właściwego poziomu ochrony przetwarzanych danych osobowych.

Mechanizmy certyfikacyjne będą miały ogromny wpływ na funkcjonowanie sektora ochrony danych osobowych. W polskim systemie prawnym z zakresu ochrony danych osobowych mechanizmy certyfikacyjne nie są znane. Nie są one jednak obce systemom prawnym innych państw członkowskich UE. Na rynku europejskim istnieje wiele podmiotów oferujących usługi certyfikacyjne komercyjnym administratorom danych osobowych. Proponowane przez te podmioty procedury certyfikacyjne nie są jednak nastawione wyłącznie na ochronę danych osobowych.

W Polsce w chwili obecnej najbliższe pojęciu certyfikacja z zakresu ochrony danych osobowych jest tworzenie wspomnianego wyżej SZBI. SZBI nie jest jednak przeznaczony do ochrony danych osobowych. Jego podstawowym celem jest ochrona zasobów informacyjnych organizacji a danych osobowych niejako przy okazji. Podejście takie zasadniczo odróżnia to rozwiązanie od certyfikacji o której mowa w RODO.

W założeniu certyfikaty wraz ze znakami jakości i oznaczeniami służącymi zademonstrowaniu zgodności z RODO maja nie tylko dać swoistą gwarancję zgodności przetwarzania danych z przepisami prawa. Mają też podnosić i utrzymywać na możliwie najwyższym poziomie ochronę danych osobowych w organizacji. RODO dzięki wprowadzeniu mechanizmów certyfikacji umożliwia budowanie możliwie najwyższego poziomu zaufania, jeżeli chodzi o sektor ochrony danych osobowych.

Kodeksy postępowania są natomiast mechanizmami pozwalającym na zdefiniowanie przez grupy instytucji (np. małe i średnie przedsiębiorstwa) lub pewne specyficzne sektory (np. instytucje zajmujące się ochroną zdrowia) list dobrych praktyk/referencji/poradników mówiących o tym, jak w najlepszy sposób w danym środowisku biznesowo – organizacyjnym wykonywać zadania związane z ochroną danych osobowych.

W swych założeniach kodeksy postępowania mają wprowadzić możliwość doprecyzowania sposobu ochrony danych osobowych z uwzględnieniem specyfiki różnych sektorów, jakie dokonują przetwarzania, co może być bardzo istotne dla podmiotów z branży medycznej.

Branżowe kodeksy postępowania, obok mechanizmów certyfikacyjnych, będą ważnym elementem realizacji nowego podejścia i wykazywania przestrzegania prawa ochrony danych.

W ocenie Izby Gospodarki Elektronicznej w Rekomendacjach powinny znaleźć się zapisy dotyczące obu ww. rozwiązań.

5) Brak informacji na temat reguł tworzenia elektronicznej dokumentacji medycznej

Jako że Rekomendacje normują kwestię rozwiązań technologicznych, które powinny być stosowane podczas przetwarzania dokumentacji medycznej w postaci elektronicznej, w ocenie Izby Gospodarki Elektronicznej dokument ten powinien zawierać informacje na temat standardu HL7 CDA.

Warto w tym miejscu wskazać, że dokumenty medyczne stosowane w medycynie winny być tworzone według ściśle określonej struktury i bazować na jednym, wiodącym wspólnym języku. Takie rozwiązanie zapewni skuteczne metody współpracy i przepływ informacji pomiędzy urządzeniami i systemami medycznymi służącymi do przetwarzania dokumentów medycznych. Dzięki temu urządzenia i systemy wykorzystywane przez placówkę medyczną do przetwarzania EDM będą kompatybilne ze sobą, ale również z urządzeniami i systemami wykorzystywanymi przez inne podmioty. Owa kompatybilność może zostać zapewniona jedynie przez **zobowiązanie** podmiotów prowadzących działalność leczniczą do stosowania Polskiej Implementacji Krajowej HL7 CDA (PIK HL7 CDA) .

Obowiązek stosowania PIK HL7 CDA przewiduje projekt ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia. W zmienianym art. 11 zaproponowano dodanie przepisu, zgodnie z którym EDM jest prowadzona przez usługodawców w formatach zamieszczonych w BIP ministra właściwego do spraw zdrowia (dodawany ust. 1a). Z kolei dodawany ust. 1b wskazuje, że usługodawcy są obowiązani dokonywać wymiany EDM, zawartej w rozporządzeniu wydanym na podstawie art. 13 ustawy, zgodnie ze standardami wymiany dokumentacji medycznej zamieszczonymi w BIP MZ.

Z uwagi na fakt, iż Rekomendacje przeznaczone są dla świadczeniodawców, którzy przetwarzają już dokumentację medyczną w formie cyfrowej, jak również dla podmiotów z branży medycznej, które dopiero przygotowują się lub też wdrażają w swoich placówkach systemy informatyczne służące do przetwarzania dokumentacji medycznej, dokument ten powinien zawierać informacje na temat PIK HL7 CDA.

6) Podsumowanie

Rekomendacje CSIOZ **w przedmiocie zapewnienia przez podmioty świadczące usługi medyczne bezpieczeństwa oraz rozwiązań technologicznych podczas przetwarzania**

elektronicznej dokumentacji medycznej są z pewnością ważnym i przydatnym dla placówek medycznych dokumentem. Z pewnością ułatwią one wdrożenie EDM w placówkach, które nie rozpoczęły jeszcze tego procesu, a także przyczynią się do usprawnienia rozwiązań stosowanych w placówkach medycznych, które dokonały już cyfryzacji dokumentacji medycznej. Niemniej, Dokument przygotowany przez CSIOZ wymaga przede wszystkim uzupełnienia w zakresie nowych obowiązków i wyzwań stojących przed administratorami danych medycznych w związku ze stosowaniem RODO. Rekomendacje powinny zwiększyć świadomość świadczeniodawców w tym przedmiocie i pomóc im przygotować się do zmian związanych z ochroną danych osobowych, które wprowadza rozporządzenie unijne. Nadto, menadżerów służby zdrowia (zwłaszcza publiczne) należy edukować w zakresie znaczenia standaryzacji w procesie budowania systemów informatycznych służących przetwarzaniu EDM. Dlatego Rekomendacje powinny zostać poszerzone o tę tematykę.

Patrycja Staniszewska
Prezes
Izby Gospodarki Elektronicznej

Olgierd Porębski
radca prawny
koordynator grupy roboczej e-zdrowie
ds. legislacyjnych