Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 355 · 2018

Informatyka i Ekonometria 13

Marek Dziembała

Uniwersytet Ekonomiczny w Katowicach
Wydział Informatyki i Komunikacji
Katedra Informatyki
marek.dziembala@ue.katowice.pl

KONCEPCJA POLITYKI BEZPIECZEŃSTWA W ŚWIETLE ZMIAN W OCHRONIE DANYCH OSOBOWYCH W PLACÓWCE MEDYCZNEJ

Streszczenie: Artykuł przedstawia koncepcję budowy polityki bezpieczeństwa danych osobowych w placówce medycznej, ze szczególnym uwzględnieniem przetwarzanych danych osobowych, w świetle zmian, które obowiązywać będą od 25 maja 2018 r. po wprowadzeniu Rozporządzenia Parlamentu Europejskiego w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. W jego ramach została opracowana koncepcja w postaci spisów treści dokumentów dostosowanych do istniejących regulacji oraz przyszłych wymogów prawnych.

Słowa kluczowe: RODO, polityka bezpieczeństwa, dane osobowe.

JEL Classification: M14.

Wprowadzenie

W związku ze zbliżającym się wymogiem dostosowania do przepisów Unijnego 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 (RODO), którego stosowanie rozpoczęło się 25 maja 2018 r., oraz z uchyleniem Dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) konieczne staje się przygotowanie organizacji na zmiany wynikające z wprowadzenia nowych przepisów.

Kształtowaniem polityki państwa w zakresie ochrony danych osobowych zajmuje się w Polsce Ministerstwo Cyfryzacji. Odpowiada ono za podjęcie działań legislacyjnych zapewniających pełne i skuteczne stosowanie ogólnego rozporządzenia w polskim porządku prawnym. Wdrażając RODO, ministerstwo udostępniło projekt nowej ustawy o ochronie danych osobowych oraz projekt zmian przepisów sektorowych obejmujący ponad 130 ustaw. Pod względem ilości zmienianych aktów prawnych projekt ten jest jednym z największych w ciągu ostatnich lat. Wdrażając nowe unijne prawo o ochronie danych osobowych, Polska stała się, w ocenie Ministerstwa Cyfryzacji, pierwszym państwem w Unii Europejskiej, które zmienia cały krajowy system prawny [www 1].

Placówki służby zdrowia, czyli zakłady opieki zdrowotnej, takie jak (zgodnie z art. 2, ust. 1 Ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej, Dz.U. z 1991 r., nr 91.91.408 z późn.zm.): szpitale, przychodnie, sanatoria, laboratoria, praktyki lekarskie, lekarsko-dentystyczne, pielęgniarskie oraz położnych, ambulatoria i inne, ze względu na charakter przetwarzanych, wrażliwych danych osobowych, zobowiązane zostały do szczególnego dostosowania procedur organizacyjnych do regulacji zawartych w RODO.

Celem artykułu jest przedstawienie koncepcji budowy polityki bezpieczeństwa, ze szczególnym uwzględnieniem przetwarzanych danych osobowych, w świetle zmian w ochronie danych osobowych w placówce medycznej. Zostaną opracowane koncepcja, spis treści, polityki bezpieczeństwa danych osobowych i niezbędne załączniki, w wyniku analizy istniejących regulacji oraz przyszłych wymogów prawnych.

1. Uwarunkowania prawne ochrony danych osobowych

Ochrona danych osobowych jest stosunkowo nową dziedziną prawa. W Unii Europejskiej Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych uregulowała sferę ochrony danych osobowych. W dniu 27 kwietnia 2016 r. Parlament Europejski i Rada (UE) wprowadziła Rozporządzenie 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), którego stosowanie rozpocznie się 25 maja 2018 r. To rozporządzenie uchyla Dyrektywę 95/46/WE. Zgodnie z zasadą pierwszeństwa prawo wspólnotowe ma wartość nadrzędną nad prawem krajowym państw członkowskich. Zasada pierwszeństwa dotyczy wszystkich aktów wspólnotowych, które mają moc wiążącą. Państwa członkowskie nie mo-

gą więc stosować przepisu krajowego, który jest niezgodny z prawem wspólnotowym.

Zauważyć należy, że w Stanach Zjednoczonych przepisy związane z ochroną danych osobowych są znacznie bardziej liberalne niż te obowiązujące w Europie. Brak jest unormowań stwarzających ogólne ramy prawne dla organizacji, które przetwarzają dane osobowe. Kwestie związane z ochroną danych osobowych można streścić następująco: co nie jest wyraźnie zabronione – jest dozwolone. A zabronione jest niewiele. Nie ma jednego urzędu, który nadzorowałby wyłącznie kwestie związane z przetwarzaniem danych osobowych. Organizacje oraz agencje rządowe w Stanach Zjednoczonych są prawdziwym potentatem, jeśli chodzi o przetwarzanie danych osobowych.

Federalne Biuro Śledcze i Urząd Imigracyjny zbierają odciski wszystkich palców u rąk oraz zdjęcie cyfrowe twarzy każdego popełniającego nawet drobne przestępstwo oraz każdego człowieka pomiędzy 14. a 79. rokiem życia, wjeżdżającego na teren Stanów Zjednoczonych Ameryki [www 2]. Przetwarzanie to obejmuje nie tylko dane obywateli USA, ale także dane osób z całego świata [www 3].

1.1. Ochrona wrażliwych danych osobowych w Polsce

W Polsce ochronę danych osobowych, a w tym danych wrażliwych, reguluje Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Polska (UODO), Dz.U. z 1997 r., nr 133, poz. 883, tekst jednolity Dz.U. z 2016 r., poz. 922, oraz 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.

Zgodnie z art. 27 ust. 1 UODO zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym w celach prawnie nieuzasadnionych. Takie dane nazywamy danymi wrażliwymi. Dane o stanie zdrowia zaliczane są więc do katalogu danych wrażliwych, które muszą podlegać szczególnej ochronie.

Ministerstwo Cyfryzacji przedstawiło projekt przepisów nowej ustawy o ochronie danych osobowych wdrażającej nowe unijne prawo o ochronie da-

nych osobowych, które zmienia cały krajowy system prawny. Projekt ten zakłada podwyższenie poziomu ochrony prywatności obywateli, w tym przyznanie im nowych, nieznanych dzisiaj i skutecznych mechanizmów ochrony przed naruszeniami, przy jednoczesnym poszanowaniu interesów przedsiębiorców.

2. Wybrane zapisy RODO odnośnie do placówek medycznych

Ochronę danych osobowych, w tym danych wrażliwych, można postrzegać dwojako – z jednej strony jako istotny element budowy zaufania użytkowników do środowiska cyfrowego, z drugiej – jako obciążenie dla organizacji. RODO wprowadza wspólną, precyzyjną i jednolicie interpretowaną terminologię danych o stanie zdrowia. Zgodnie z art. 4 pkt 15 RODO „dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

W motywie 35. preambuły twórcy rozporządzenia RODO wyjaśniają, że: „do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE (1); numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; 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".

Dodatkowo motyw 74. preambuły nakłada: „na administratora obowiązki i ustanawia odpowiedzialność prawną administratora za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. W szczególności administrator powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z niniejszym rozporządzeniem oraz że są skuteczne. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia

praw i wolności osób fizycznych", a w motywie 78. czytamy: „Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów niniejszego rozporządzenia. Aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń. Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych".

Zapisom prawa w RODO została nadana taka forma, która pozwala dostosować je do zmieniającej się rzeczywistości. Czytając zapisy w przytoczonych motywach, trudno jest sobie wyobrazić, żeby te zapisy się zdezaktualizowały, niezależnie od tego, w którym kierunku będzie podążał rozwój technologii.

Dzisiaj obywatele, zwłaszcza pacjenci, często mają poczucie, że ich dane osobowe nie są wystarczająco chronione, dlatego ograniczają przekazywanie organizacjom swoich danych. Na ich podstawie możliwe jest jednak świadczenie usług jeszcze bardziej innowacyjnych i wygodnych dla obywateli, na przykład związanych z telemedycyną, ale pacjent musi mieć absolutną gwarancję, że jego dane będą wykorzystane tylko w celu, w którym zostały zebrane.

3. Koncepcja budowy polityki bezpieczeństwa zgodnej z zapisami RODO

RODO wprowadza dla pacjentów szereg nowych uprawnień, a na administratora danych nowe obowiązki, m.in.:

- ochrona danych osobowych niezależnie od miejsca ich przetwarzania,
- konieczność powołania Inspektora Ochrony Danych,

- ustanowienie systemu monitorowania, przeglądu i oceny procedur przetwarzania danych osobowych,
- minimalizowanie przetwarzania i przechowywania danych osobowych,
- wdrożenie środków ochronnych przy przetwarzaniu danych,
- dokumentowanie zasad, procedur i czynności przetwarzania danych osobowych, które muszą być możliwe do udostępnienia organom nadzorczym na ich wniosek,
- ocenianie ryzyka i wpływu zamierzonego przetwarzania na prywatność pacjentów,
- uzyskanie zgody konsumenta na przetwarzanie danych osobowych, która musi być dobrowolna i świadoma oraz musi wskazywać cel przetwarzania danych,
- konieczność poinformowania pacjentów o przysługującym im prawie do wycofania swojej zgody, a jej wycofanie musi być równie łatwe, jak jej wyrażenie,
- formułowanie klauzul służących do odbierania zgody czytelnym językiem, także zrozumiałym dla dziecka,
- pozyskanie „wyraźnej" zgody, szczególnie w przypadku wrażliwych danych osobowych lub transgranicznego przepływu danych,
- poprzedzenie uzyskania zgody jasną informacją o podstawach prawnych, celu i innych aspektach przetwarzania danych,
- zgłaszanie przez placówki medyczne organowi nadzorczemu naruszenia danych osobowych do 72 godzin od ich stwierdzenia; osoby, których dotyczy naruszenie, będą musiały być poinformowane o incydencie,
- wdrożenie Prawa do bycia zapomnianym,
- wdrożenie Prawa do przenoszenia danych,
- wdrożenie Prawa do sprzeciwu wobec profilowania,
- uwzględnienie ochronych danych przy rozwijaniu procesów biznesowych i nowych systemów już na etapie projektowania usług, systemów i aplikacji,
- ustawienie opcji prywatności domyślnie na wysokim poziomie, bez konieczności ingerencji użytkownika,
- umożliwienie podziału odpowiedzialności za ochronę danych osobowych między kilku różnych współadministratorów danych; obowiązek ochrony danych obejmuje również podmioty przetwarzające dane na zlecenie.

W rozporządzeniu nie ma zapisów wprowadzających formalny obowiązek prowadzenia dokumentacji przetwarzania danych osobowych przez wszystkich administratorów danych. Jednak zgodnie z nim, aby wykazać, że jego regulacje są przestrzegane, administrator danych powinien przyjąć wewnętrzne polityki

bezpieczeństwa i wdrożyć odpowiednie środki, by zapewnić skuteczną ochronę danych osobowych. W razie kontroli taką politykę będzie mógł przedstawić organowi nadzorczemu, wykazując, że zostały wdrożył odpowiednie środki w celu skutecznej ochrony danych osobowych.

Taka Polityka Bezpieczeństwa to jeden z podstawowych dokumentów, który dowodzi, że przetwarzanie danych odbywa się zgodnie z prawem. Pozwala ona zapewnić, że pracownicy są świadomi, jakie mają obowiązki w zakresie przetwarzania danych osobowych, wskazuje się w niej, że administrator danych wdrożył odpowiednie środki techniczne i organizacyjne na różnych poziomach organizacji [Białas, 2007, s. 166], aby skutecznie chronić dane osobowe.

Przed wdrożeniem nowych rozwiązań polskie przepisy zobowiązywały administratora danych do wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych. Wydaje się więc właściwym opieranie się na prowadzonej dotychczas dokumentacji. Dostosowanie jej do wymagań RODO musi objąć dostosowanie treści dokumentów do sposobu przetwarzania i środków ochrony danych stosowanych w danej placówce medycznej. Unijny regulator pozostawił kierownictwu organizacji dostosowanie struktury, rodzajów i liczby dokumentów do realnych potrzeb.

Koncepcja budowy dokumentacji zgodnej z RODO opiera się Polityce Ochrony Danych Osobowych oraz na Instrukcji Zarządzania Systemem Informatycznym. Dostosowano treść poszczególnych rozdziałów Polityki oraz Instrukcji, wprowadzając wymagane RODO zapisy, które muszą być uwzględnione w istniejących procesach biznesowych placówki medycznej.

Polityka Bezpieczeństwa powinna zawierać:

- Wykaz podstawowych skrótów,
- Wykaz podstawowych definicji,
- Wprowadzenie,
- Strategię bezpieczeństwa,
- Cele Polityki Bezpieczeństwa Danych Osobowych,
- Zadania Inspektora Ochrony Danych,
- Procedura zarządzania zmianą / zarządzania projektami (Privacy by Design),
- Sposób monitorowania i reagowania na naruszenia ochrony danych,
- Sposób zarządzania ryzykiem utraty prywatności (Privacy Impact Assessment lub Data Protection Impact Assessment),
- Podstawowe zasady ochrony danych osobowych,
- Upoważnienie do przetwarzania danych osobowych,
- Egzekwowanie prawa do bycia zapomnianym,
- Egzekwowanie prawa do przenoszenia danych,

- Egzekwowanie prawa do sprzeciwu wobec profilowania,
- Powierzenie przetwarzania danych osobowych,
- Udostępnianie danych osobowych, w tym przekazywanie danych osobowych poza Polskę,
- Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
- Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- Opis sposobu przepływu danych pomiędzy poszczególnymi systemami,
- Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
- Rejestr incydentów i zdarzeń, zgłaszanie naruszenia ochrony danych,
- Rejestr operacji przetwarzania danych osobowych,
- Rejestr osób upoważnionych do przetwarzania danych osobowych,
- Plan audytu i szkoleń pracowników,
- Przepisy karne i porządkowe,
- Postanowienia końcowe,
- Opis struktury zbiorów danych osobowych,
- Wzory klauzul informacyjnych i oświadczeń,
- Raport z analizy (Privacy Impact Assessment lub Data Protection Impact Assessment),
- Instrukcję kancelaryjną.

Instrukcja Zarządzania Systemem Informatycznym powinna zawierać:

- Wykaz podstawowych skrótów,
- Wykaz podstawowych definicji,
- Wprowadzenie,
- Zakres stosowania Instrukcji Zarządzania Systemami Informatycznymi,
- Standardy zabezpieczeń,
- Procedurę nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym,
- Stosowane metody i środki uwierzytelniania oraz procedury związanych z ich zarządzaniem i użytkowaniem,
- Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym,
- Zabezpieczenie nośników informacji zawierających dane osobowe,
- Kopie zapasowe oraz sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe,

- Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania,
- Realizację wymogów, o których mowa w §7, ust. 1, pkt. 4 Rozporządzenia MSWIA,
- Instrukcję wykonywania przeglądów i konserwacji systemów informatycznych.

Nadmienić należy, że nawet gdy proces wdrażania dokumentacji zgodnej z RODO się zakończy, powinna ona być na bieżąco weryfikowana pod względem zmieniającego się otoczenia prawnego i biznesowego oraz udoskonalana w zależności od potrzeb.

Podsumowanie

Przedstawiona struktura dokumentów wydaje się konkretną propozycją do zastosowania w większości placówek medycznych. Autor, w ramach prowadzonych badań, zaproponował wdrożenie przedstawionej dokumentacji do wybranego szpitala. Proces wypełnienia treścią poszczególnych rozdziałów oraz modernizacji istniejących treści jest bardzo czasochłonny i dotyka wszystkich jednostek organizacyjnych szpitala. Wymaga reorganizacji istniejących procesów biznesowych podstawowych i pomocniczych, a także ponownych szkoleń wszystkich pracowników. Zmiana dotyka procesów związanych z wykonywaniem konkretnych świadczeń medycznych, co wymaga szczególnej uwagi. W oparciu o zaproponowaną dokumentację można wyznaczyć kolejne kroki, które należy wykonać, aby dostosować placówkę medyczną do wymagań RODO.

Literatura

Białas A. (2007), *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

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, Dz.U. z 2004 r., nr 100, poz. 1024.

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).

Ustawa z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej, Dz.U. z 1991 r., nr 91.91.408 z późn.zm.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Polska (UODO), Dz.U. z 1997 r., nr 133, poz. 883, tekst jednolity Dz.U. z 2016 r., poz. 922.

[www 1] https://www.gov.pl/cyfryzacja/nowe-prawo-ochrony-danych-osobowych (dostęp: 9.02.2018).

[www 2] https://archives.fbi.gov/archives/news/testimony/fbi-fingerprint-program (dostęp: 09.02.2018).

[www 3] https://www.immihelp.com/ visas/usvisit.html (dostęp: 09.02.2018).

CONCEPT OF INFORMATION POLICY IN THE LIGHT OF CHANGES IN THE PROTECTION OF PERSONAL DATA IN HEALTH CARE

Summary: The article presents the concept of building a personal data security policy in a medical facility, with particular emphasis on personal data being processed, in the light of changes that will apply from 25 May 2018 after the introduction of the European Parliament Regulation on the protection of individuals with regard to the processing of personal data and on the free movement such data. A concept, specific tables of contents of documents adapted to existing regulations and future legal requirements were developed.

Keywords: GDPR, information policy, personal data.