Dr Artur Romaszewski
Uniwersytet Jagielloński Collegium Medicum
Wydział Nauk o Zdrowiu, Zakład Medycznych Systemów Informacyjnych
artur.romaszewski@uj.edu.pl

Mgr Mariusz Kielar
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu, Zakład Medycznych Systemów Informacyjnych
krzysztof.gajda@uj.edu.pl

Mgr Krzysztof Gajda
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu, Zakład Medycznych Systemów Informacyjnych
mariusz.kielar@uj.edu.pl

Dr hab. Wojciech Trąbka
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
Wydział Lekarski i Nauk o Zdrowiu, Katedra Bioinformatyki i Zdrowia Publicznego
wojciech.trabka@uj.edu.pl

BEZPIECZEŃSTWO DANYCH OSOBOWYCH W SYSTEMIE OCHRONY ZDROWIA – NIE TYLKO RODO

Wprowadzenie

W związku ze zmianami regulacji prawnych dotyczących ochrony danych osobowych spowodowanymi przede wszystkim wejściem w życie 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[1] (ogólne rozporządzenie o ochronie danych) zwanego dalej w tekście RODO, ukazało się szereg publikacji opisujących ten problem, w tym także jego reperkusje w ochronie zdrowia. Jednak zdaniem autorów publikacji problem jest bardziej złożony i trudno rozważać RODO w oderwaniu od innych regulacji, które w bardzo dużym stopniu będą wpływały na funkcjonowanie podmiotów leczniczych. Część zagadnień dotyczących tematyki bezpieczeństwa, związanych z wprowadzeniem ważnych regulacji Unii Europejskiej (UE) oraz uzupełniających ich aktów prawa krajowego, w odniesieniu do systemu ochrony zdrowia jest bardzo rzadko publicznie

[1] 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), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32016R0679 (data dostępu: 06.2018).

poruszana. Mowa tutaj przede wszystkim o regulacji wprowadzającej jednolite narzędzia służące do bezpiecznego tworzenia dokumentów elektronicznych dzięki powołaniu do życia w UE usług zaufania publicznego.

Zapewnieniu bezpiecznej identyfikacji wszystkich podmiotów uczestniczących w wymianie informacji w sieciach teleinformatycznych oraz uwierzytelnianiu serwerów przechowujących ważne informacje mają służyć przepisy eIDAS oraz polskie regulacje będące ich uzupełnieniem[2]. Nie mniej istotne są przepisy, które w ochronie zdrowia - sektorze niezwykle ważnym dla funkcjonowania kraju - będą wskazywały odpowiednich dostawców usług internetowych. Dodatkowo od lat funkcjonują przepisy narzucające wymóg wdrożenia odpowiednich standardów dla wszystkich podmiotów wymieniających się informacją z instytucjami publicznymi. Wymiana dokumentów elektronicznych została prawnie uregulowana i powinna funkcjonować również w ochronie zdrowia, zgodnie z wymogami prawa.

W chwili tworzenia tekstu opublikowano projekt Rozporządzenia UE *e-Privacy*, który będąc regulacją *lex specialis* do RODO ma zapewnić bezpieczeństwo danych nie tylko osobom fizycznym, ale również prawnym. Niezwykle ważne jest również przyjęcie Dyrektywy NIS[3], w rezultacie której sektor ochrony zdrowia będzie musiał wybierać m.in. operatorów usług cyfrowych (w tym np. dostawców chmury obliczeniowej) spośród wskazanych przepisami prawa (Rysunek 1). Nową regulacją, która wpłynie na bezpieczeństwo danych przetwarzanych w podmiocie leczniczym, jest Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem i jej implementacja tej regulacji do polskiego systemu prawa[4]. Zawiera ona nowe ujęcie problemu tajemnicy przedsiębiorstwa w Dyrektywie UE[5].

Celem niniejszego artykułu jest uporządkowanie i wprowadzenie pewnej systematyki do problemu bezpieczeństwa danych przetwarzanych w podmiotach leczniczych.

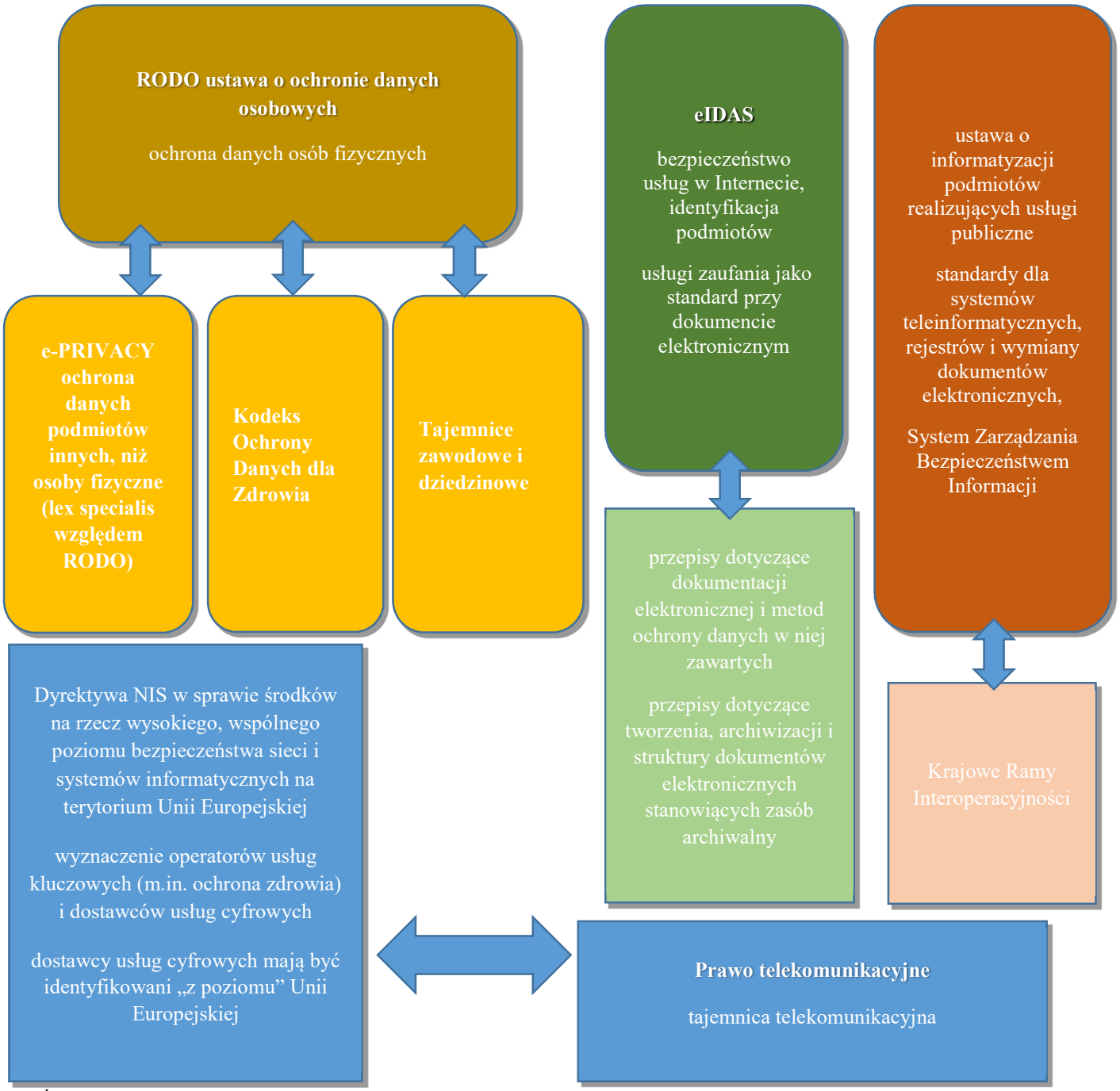
[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (eIDAS) oraz ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej Dz.U. 2016 poz. 1579.
[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej.*
[4] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 9 lutego 2018 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zwalczaniu nieuczciwej konkurencji Dz.U. 2018 poz. 419
[5] R. Solga, Dyrektywa UE dotycząca tajemnicy przedsiębiorstwa i know-how, https://tajemnica-przedsiebiorstwa.pl/dyrektywa-ue-tajemnica-przedsiebiorstwa-i-know-how/ (data dostępu: 06.2018).

1. Problemy ochrony danych pacjentów w aspekcie RODO

Szum medialny, który był związany z wdrożeniem przepisów RODO, spowodował dużą nerwowość wszystkich środowisk medycznych - nawet tych, które od lat poprawnie uregulowały w swoich podmiotach procedury bezpiecznego przetwarzania danych.

Grupy regulacji dotyczących bezpieczeństwa danych i dokumentów w ochronie zdrowia przedstawia Rysunek 1.

Rysunek 1. Grupy regulacji dotyczących bezpieczeństwa danych i dokumentów w ochronie zdrowia



Źródło: Opracowanie własne.

Duża bowiem część podmiotów nie wprowadza niczego nowego, natomiast modyfikuje swoje, tworzone na podstawie dotychczas obowiązujących regulacji, systemy ochrony danych osobowych[6,7].

Oczywiście należy wprowadzić wymagane prawem zmiany. Pamiętać jednak należy, żeby zweryfikować i uaktualnić rozwiązania dotychczasowe pod kątem spełniania przez nie wymogów RODO (po wszechstronnej analizie). Obowiązująca obecnie w UE regulacja dotycząca ochrony danych różni się od dotychczas obowiązujących przepisów tym, że nie narzuca konkretnych rozwiązań wszystkim instytucjom i osobom przetwarzającym dane osobowe, zobowiązując podmioty do stworzenia swoich wewnętrznych modeli zapewniających ich bezpieczeństwo i poufność.

W każdym podmiocie świadczącym usługi medyczne administrator danych - uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia - wdraża odpowiednie środki techniczne i organizacyjne, dbając jednocześnie o to, aby móc to udokumentować. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane[8].

2. Specyfika danych medycznych i instytucji opieki zdrowotnej – brak jednolitego modelu systemu bezpieczeństwa

Trzeba jasno powiedzieć, że nie da się stworzyć szablonu, na podstawie którego będą tworzone modele bezpieczeństwa danych osobowych. Działania podjęte w każdym podmiocie można wspierać i proponować pewne określone rozwiązania, natomiast inne rozwiązania są wymuszane przez specyfikę firm medycznych. Nie rozwiąże również tego problemu przyjęcie i wdrożenie kodeksu bezpieczeństwa danych osobowych w ochronie zdrowia[9].

Specyfika ta jest wynikiem wielu czynników. Przede wszystkim jest związana z kształtowaniem się rynku usług medycznych pod koniec lat 90-tych XX wieku. Podmioty

[6] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz.U. 1997 nr 133 poz. 883.
[7] 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. 2004 nr 100 poz. 1024.
[8] *Artykuł 24* 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).
[9] http://www.rodowzdrowiu.pl (data dostępu: 06.2018).

medyczne powstawały często w wyniku przekształceń SPZOZ-ów w zakłady niepubliczne. Inne były tworzone od podstaw. Podmioty niepubliczne tworzone w wyniku przekształceń często przejmowały zarówno pacjentów, jak też dokumentację medyczną przechowywaną w archiwach podmiotów publicznych. Przejmowana była też dokumentacja (często archiwalna) pracowników i osób świadczących usługi na podstawie umów cywilnoprawnych. Przez lata zmieniały się również zakresy świadczonych usług - część świadczonych usług kontynuowano, część wygaszano, a także w zależności od zapotrzebowania pojawiały się nowe usługi.

Podmioty funkcjonujące na rynku stosunkowo krótko (a więc od czasu, kiedy została dopuszczona taka możliwość) mogły od początku istnienia prowadzić dokumentację w postaci elektronicznej, bez bagażu przechowywania papierowych archiwów. Mogły również prowadzić dokumentację medyczną z wykorzystaniem zasobów chmurowych, co powodowało, że bezpieczeństwo danych przetwarzanych w podmiocie przejmował na podstawie umowy podmiot zewnętrzny.

Skutkiem powyżej przedstawionej sytuacji jest to, że podmioty lecznicze przetwarzają różne zbiory danych medycznych, zarówno na nośnikach papierowych, jak też elektronicznych. Wśród danych przetwarzanych przez podmioty lecznicze znajdują się zarówno tzw. zwykłe dane osobowe, jak i „szczególne kategorie danych" (tzw. dane wrażliwe). Przetwarzane są także różne typy danych m.in. tekstowe, video, mp3, generowane w trakcie diagnostyki obrazowej, zarówno na ostrych kliszach RTG, jak i w postaci plików cyfrowych. Wśród danych przetwarzanych przez podmioty świadczące usługi medyczne największą grupę stanowią dane i informacje dotyczące samych pacjentów, jak i ich stanu zdrowia. W tej grupie jednak nie wszystkie dane to dane wrażliwe, których przetwarzanie jest szczególnie chronione.

Wśród tych danych znajdują się również dane teleadresowe, które po uzyskaniu zgody pacjenta można wykorzystywać np. w celach marketingowych.

Dane osobowe są gromadzone w zbiorach. Zbiór danych to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie[10]. Obok zbiorów dotyczących pacjentów można wyodrębnić m.in. zbiory pracowników, osób świadczących usługi na podstawie umowy cywilnoprawnej, zbiory

[10] Art. 4 pkt. 6 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).

zawierające osoby składające skargi i wiele innych. Trzeba pamiętać, że każdy z tych zbiorów powinien być wykazany w dokumentacji firmy.

Każdy podmiot leczniczy powinien dokonać oceny zasobów i zadecydować, jakie działania organizacyjne i techniczne należy podjąć w stosunku do poszczególnych zbiorów. Trzeba pamiętać o zasadach uregulowanych w RODO: zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu przetwarzania danych, minimalizacji danych, prawidłowości danych, ograniczenia przechowywania danych, integralności i poufności oraz rozliczalności.

Tworząc model ochrony i dokonując oceny dotychczas funkcjonującego trzeba przeanalizować dotychczas stosowane rozwiązania. Pojawiają się bowiem doniesienia o tym, że niektóre rozwiązania udostępniające zasoby on-line mogą stwarzać zagrożenia. W związku z tym niezbędny jest proces analizy ryzyka. Ostatnio pojawiły się doniesienia o możliwości uzyskania dostępu do wyników badań online, na podstawie faktur wystawianych za przeprowadzone badanie lub na podstawie przewidywalnego numeru laboratoryjnego[11].

3. Podstawowe zasady przetwarzania danych osobowych w odniesieniu do systemu opieki zdrowotnej

Zasada zgodności z prawem, rzetelności i przejrzystości - w praktyce zasada ta będzie realizowana poprzez spełnienie przez administratora obowiązków informacyjnych względem osób, których dane dotyczą. Przejrzystość ma na celu zbudować zaufanie do procesów dotyczących obywateli umożliwiając im zrozumienie oraz – w razie konieczności - zakwestionowanie tych procesów. Dla osób fizycznych powinno bowiem być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane.

Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Dostępność ta oznacza, że osoba, której dane dotyczą, nie powinna być zmuszona do poszukiwania informacji. Dla takiej osoby powinno być oczywiste, gdzie i w jaki sposób taka informacja może być dostępna - na przykład poprzez jej bezpośrednie

[11] M. Maj, *Jak niektóre placówki medyczne udostępniają dane pacjentów przez Internet*. Niebezpiecznik, https://niebezpiecznik.pl/post/odbierales-swoje-badania-lekarskie-przez-internet-mamy-nadzieje-ze-nie-w-taki-sposob/ (data dostępu: 06.2018).

dostarczenie, dostarczenie linka do takiej informacji, poprzez jej jasne oznaczenie lub jako odpowiedź na zapytanie sformułowane zwykłym językiem[12].

Prawidłowa realizacja obowiązków informacyjnych jest zatem warunkiem niezbędnym dla osiągnięcia zgodności z zasadą rzetelności i przejrzystości. Na jej podstawie administrator danych musi zagwarantować poprawność i aktualność zgromadzonych danych osobowych, oraz że ich przetwarzanie odbywa się bez utrudnień. Do jego obowiązków należy więc m. in. wdrożenie środków technicznych i organizacyjnych umożliwiających korektę danych, zmniejszenie ryzyka błędów oraz usunięcie nieprawidłowych danych. Ten ostatni aspekt ma kluczowe znaczenie w przypadku stosowania tzw. mechanizmu profilowania – ewentualne nieprawidłowości w zakresie danych osobowych, przy braku możliwości ich modyfikacji, mogą prowadzić do ryzyka po stronie interesów i praw osoby, której dane te dotyczą. W przypadku wprowadzenia zmian lub uzupełnień do takich informacji administratorzy powinni jasno zakomunikować osobom, których dane dotyczą, że takie zmiany zostały przeprowadzone w celu zastosowania się do GDPR. Grupa Robocza Art. 29 zaleca, by w sposób aktywny zwrócono uwagę osób, których dane dotyczą, na takie zmiany lub uzupełnienia. Warunkiem minimum, jaki administratorzy powinni spełnić, jest to, by taka informacja była powszechnie dostępna (np. na stronie internetowej).

W praktyce spełnienie tej zasady sprowadza się do dokonania rzetelnego przeglądu obowiązujących w placówce polityk ochrony danych, zasad postępowania oraz szkoleń pracowników w zakresie zgodności w omawianą zasadą. Konieczna jest przy tym implementacja właściwych funkcjonalności wspomagających powyższe elementy na poziomie baz danych oraz aplikacji obsługujących te bazy[13].

Zasada ograniczenia celu - cel przetwarzania danych musi być wyraźnie określony w momencie ich pozyskania, prawnie uzasadniony oraz niemożliwy do osiągnięcia przy użyciu innych sposobów. Gdy przetwarzanie danych opiera się na podstawie zgody, jej zakres odnosi się jedynie do konkretnie wskazanego celu przetwarzania - nowy cel przetwarzania danych wymaga pozyskania nowej zgody. Warunkiem kontynuacji przetwarzania danych na dotychczasowych zasadach jest jednak pozostawanie nowego celu w zgodności z pierwotnym. Niezależnie od zgodności (lub jej braku) nowego celu przetwarzania danych z celem

[12] Wytyczne w sprawie przejrzystości na mocy rozporządzenia 2016/679, Grupa Robocza Artykułu 29, https://gdpr.pl/wytyczne-grupy-roboczej-art-29-sprawie-przejrzystosci-mocy-rozporzadzenia-2016679 (data dostępu: 06.2018).
[13] https://www.giodo.gov.pl/1520285 (data dostępu: 06.2018).

pierwotnym, konieczne jest poinformowanie osoby, której dane dotyczą, o zmianie takiego celu. Obowiązek informowania osób o celach przetwarzania ich danych osobowych pozostaje w gestii administratora danych. Wyjątkiem są tu sytuacje, w których dane osobowe są przechowywane przez administratora w celach archiwalnych mimo, że pierwotny cel przetwarzania takich danych nie jest aktualny. Regulacje RODO dopuszczają taką możliwość, nie tylko na potrzeby archiwizacji, lecz również gdy przemawia za takim postępowaniem interes publiczny, cele badań naukowych lub historycznych oraz cele statystyczne, w przypadku których dalsze przetwarzanie danych nie uznaje się za niezgodne z pierwotnymi celami.

Zasada minimalizacji danych – zakres przetwarzanych danych powinien być taki, jaki jest niezbędny do osiągnięcia określonego celu przetwarzania danych. Innymi słowy, każdy podmiot przetwarzający dane musi dokonać selekcji danych wybierając tylko taką ich ilość oraz rodzaj, jakie są dla niego niezbędne. Istotne jest również ograniczenie okresu przechowywania danych. Praktyczna realizacja tej zasady powinna polegać na precyzyjnym - jeszcze przed rozpoczęciem przetwarzania danych osobowych – przyporządkowaniu celów oraz odpowiadających im rodzajów danych oraz ustaleniu terminu usuwania i okresowej weryfikacji danych. W myśl przedmiotowej zasady także zakres nadawanych uprawnień dostępu do informacji powinien być minimalny, aby osiągnąć cel ich przetwarzania. Niestety w przypadku placówek medycznych takie postępowanie nie zawsze jest respektowane – wielokrotnie przydzielany jest dostęp do pełnego zakresu informacji dla osób, które niekoniecznie wymagają go do wykonywania swoich zadań.

Zasada prawidłowości danych – w praktyce oznacza, że powinny być stworzone odpowiednie rozwiązania techniczne oraz organizacyjne umożliwiające korygowanie nieprawidłowych lub nieaktualnych danych. Powyższa zasada nawiązuje do stanowiska Komisji Europejskiej wyrażonego w komunikacie z dnia 4 listopada 2010 r., zgodnie z którym osoba, której dane dotyczą, powinna zawsze mieć możliwość wglądu w swoje dane, poprawiania błędnych danych, żądania usunięcia ich, a także wstrzymania przetwarzania danych, chyba że istnieją prawnie uzasadnione powody, aby działania takie osobie fizycznej uniemożliwić[14].

[14] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów z dnia 4 listopada 2010 r., *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*, COM(2010) 609, s. 8.

Zasada ograniczenia przechowywania – stanowi, iż forma i okres przetwarzania danych musi być ograniczony do czasu, jaki jest niezbędny do tego, aby osiągnąć założony cel przetwarzania danych**.** Tym samym powstaje zobowiązanie administratora danych do określenia, w miarę możliwości, planowych terminów usunięcia poszczególnych kategorii danych zamieszczonych w rejestrze czynności przetwarzania danych osobowych prowadzonych przez administratora danych lub jego przedstawiciela. Konstrukcja zapisu prawnego zakłada zatem podejście indywidualne, przewidując sytuację, w której nie jest możliwe określenie terminu usunięcia danych. Dopuszcza zatem w określonych przypadkach możliwość przetwarzania danych przez niesprecyzowany okres czasu, o ile nie została naruszona zasada celowości.

Zasada integralności i poufności – integralność nakłada na administratora danych obowiązek przetwarzania danych gwarantujący odpowiedni poziom bezpieczeństwa. Natomiast poufność ma na celu zapobieganie sytuacjom, w którym dane osobowe są udostępniane lub ujawniane nieautoryzowanym podmiotom, czy procesom. W praktyce realizacja obydwu tych postulatów polega na przeprowadzeniu analizy ryzyka zakresu przetwarzania danych i charakteru danych podlegających ochronie oraz następowym wdrożeniu odpowiednich środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych. Są one konieczne, aby dane osobowe były przetwarzane z zapewnieniem odpowiedniego poziomu bezpieczeństwa danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem, nieautoryzowanym przetwarzaniem oraz ochronę przed przypadkową utratą, zniszczeniem lub uszkodzeniem.

Zasada rozliczalności – zgodnie z nią administrator danych będzie musiał wykazać, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne. Tym samym administrator danych powinien być w stanie wykazać zgodność i skuteczność stosowanych przez siebie metod przetwarzania danych. Sposobem praktycznej realizacji zasady rozliczalności może być implementacja procedur inwentaryzacyjnych i prowadzenie rzetelnej dokumentacji sprawozdawczej, która potwierdzałaby spełnienie przewidzianych wymogów.

Warto zwrócić uwagę, że wszystkie zbiory danych osobowych powinny być wykazane w dokumentacji, której prowadzenie wymagały poprzednie przepisy – polityka bezpieczeństwa prowadzona m.in. w celu inwentaryzacji wszelkich zasobów zbiorów danych. Część zbiorów oprócz tego, że była wykazywana, to dodatkowo była zgłaszana do GIODO. Jeżeli natomiast

instytucja powoływała administratora bezpieczeństwa informacji (ABI) to podlegała wpisowi do prowadzonego przez niego rejestru[15].

4. Dokumentacja systemu zabezpieczenia danych w podmiotach leczniczych

Obecnie RODO nie narzuca rozwiązań dotyczących dokumentacji bezpieczeństwa. Administrator danych samodzielnie ocenia, jakie środki techniczne i organizacyjne są właściwe, aby móc udowodnić i wykazać, że dane osobowe są przetwarzane zgodnie z prawem. Nie narzuca standardów i innych wymagań technicznych. Wymaga natomiast wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów Rozporządzenia.

Aby móc wykazać przestrzeganie przepisów, administrator danych powinien przyjąć wewnętrzne polityki. Jeżeli szacując ryzyko na podstawie obiektywnej oceny[16] administrator danych uzna, że dotychczas stosowane środki i metody ochrony są wystarczające i dotychczas obowiązujące zasady są wystarczające, to nie ma przeszkód, żeby obydwa dokumenty (tzn. politykę bezpieczeństwa oraz zawierającą uregulowane procedury postepowania przy przetwarzaniu danych (instrukcję zarządzania systemem informatycznym) włączyć do tworzonego systemu bezpieczeństwa. Oczywiście będą one wymagały weryfikacji i aktualizacji w takim zakresie, jaki jest niezbędny, aby ich zapisy były adekwatne do zakresu i sposobu przetwarzanych przez nich w podmiocie danych osobowych[17].

Szczególnie należy zweryfikować wymagane poprzednio, określone dla każdego podmiotu, poziomy ryzyka jako niski, średni i wysoki, które uzależnione były od rodzaju danych i podłączenia urządzeń do Internetu. W zależności od przyjętego poziomu należało wdrożyć odpowiednie zabezpieczenia. Należy pamiętać, że niektóre wymagane w podmiocie leczniczym dokumenty, które możemy dołączyć do szeroko rozumianego systemu ochrony danych, wynikają również z innych niż RODO regulacji (np. z ustawy o prawach pacjenta).

Można przyjąć, że zgodnie z RODO - obok omówionej powyżej dokumentacji stworzonej na podstawie obowiązujących do czasu zmiany przepisów tj. polityki bezpieczeństwa i

[15] https://gdpr.pl/wp-content/uploads/2018/06/Belgia_Zalecenie_w_sprawie_Rejestru_czynno%C5%9Bci_przetwarzania_danych.pdf (data dostępu: 06.2018).
[16] Motyw 76, RODO.
[17] *Co zrobić z Polityką bezpieczeństwa obowiązującą w firmie po wejściu w życie RODO? Prawo czy lewo?*, https://swks.com.pl/blog/ (data dostępu: 06.2018).

instrukcji zarządzania systemami informatycznymi, w podmiocie leczniczym będą musiały być prowadzone następujące dokumenty:

1. Rejestr Czynności Przetwarzania Danych Osobowych - jeżeli podmiot jest administratorem lub Rejestr Wszystkich Kategorii Czynności Przetwarzania Dokonywanych w Imieniu Administratora - dotyczy podmiotu przetwarzającego,
2. dokumentacja dotycząca wszelkich naruszeń ochrony danych osobowych,
3. wzory klauzul zgód na przetwarzania danych osobowych,
4. wzory klauzul informacyjnych na przetwarzanie danych osobowych,
5. wzór umowy na przetwarzanie danych osobowych lub wzór umowy o współadministrowaniu (o ile są potrzebne),
6. rejestr upoważnień na przetwarzanie danych osobowych i wzór upoważnienia na przetwarzanie danych osobowych,
7. procedurę w przypadku naruszenia ochrony danych osobowych i rejestr naruszeń ochrony danych osobowych,
8. procedurę prostowania i usuwania danych osobowych[18],
9. rejestr sprzeciwów wobec przetwarzanych danych,
10. wykaz zawierający informacje dotyczące udostępnianej dokumentacji medycznej[19]
11. wykaz osób wykonujących czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna i zapewnieniem bezpieczeństwa tego systemu, na podstawie upoważnienia administratora danych,
12. wykaz osób wykonujących zawód medyczny mających dostęp do dokumentacji osób innych niż pacjenci danej osoby[20].

Oczywiście powyższy wykaz dokumentacji jest przykładowy i zakłada samodzielność wyboru ze strony administratora danych.

[18] P. Ludwiczak, *Dokumentacja zgodna z RODO*, http://samorzad.infor.pl/sektor/organizacja/rodo-2018/780354,Dokumentacja-zgodna-z-RODO.html (data dostępu: 06.2018).
[19] Art. 27 ust.4 Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, Dz.U. 2009 nr 52 poz. 417.
[20] Ibidem.

Podsumowanie

Obowiązująca obecnie w UE regulacja dotycząca ochrony danych różni się od dotychczas obowiązujących przepisów tym, że nie narzuca konkretnych rozwiązań wszystkim instytucjom i osobom przetwarzającym dane osobowe, zobowiązując podmioty do stworzenia swoich wewnętrznych modeli zapewniających ich bezpieczeństwo i poufność. W każdym podmiocie świadczącym usługi medyczne administrator danych - uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia - wdraża odpowiednie środki techniczne i organizacyjne, dbając jednocześnie o to, aby móc to udokumentować.

Specyfika danych medycznych oraz systemu funkcjonowania instytucji opieki zdrowotnej stawia dodatkowe wyzwania przed systemami przetwarzającymi dane medyczne oraz powoduje brak jednolitego modelu systemu bezpieczeństwa.

Określone zostały podstawowe zasady przetwarzania danych osobowy, które musza być zastosowane w odniesieniu do danych medycznych: Zasada zgodności z prawem, rzetelności i przejrzystości; zasada ograniczenia celu; zasada minimalizacji danych; zasada prawidłowości danych; zasada ograniczenia przechowywania; zasada integralności i poufności oraz zasada rozliczalności.

Nie można rozważać regulacji związanych z RODO bez uwzględnienia regulacji wprowadzającej jednolite narzędzia służące do bezpiecznego tworzenia dokumentów elektronicznych dzięki powołaniu do życia w UE usług zaufania publicznego oraz identyfikacji wszystkich podmiotów uczestniczących w wymianie informacji w sieciach teleinformatycznych oraz uwierzytelnianiu serwerów.

Literatura

[1] *Co zrobić z Polityką bezpieczeństwa obowiązującą w firmie po wejściu w życie RODO? Prawo czy lewo?*, https://swks.com.pl/blog/.
[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej.*
[3] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów z dnia 4 listopada 2010 r., *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*, COM(2010) 609, s. 8.
[4] Ludwiczak P., *Dokumentacja zgodna z RODO*, http://samorzad.infor.pl/sektor/organizacja/rodo-2018/780354,Dokumentacja-zgodna-z-RODO.html.

[5] Maj M., *Jak niektóre placówki medyczne udostępniają dane pacjentów przez Internet*. Niebezpiecznik, https://niebezpiecznik.pl/post/odbierales-swoje-badania-lekarskie-przez-internet-mamy-nadzieje-ze-nie-w-taki-sposob/.
[6] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 9 lutego 2018 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zwalczaniu nieuczciwej konkurencji Dz.U. 2018 poz. 419.
[7] 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. 2004 nr 100 poz. 1024.
[8] 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), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32016R0679.
[9] Rozporządzenie Parlamentu Europejskiego i Rady *w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do e-transakcji na rynku wewnętrznym,* Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej Dz.U. 2016 poz. 1579.
[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (eIDAS).
[11] Solga R., Dyrektywa UE dotycząca tajemnicy przedsiębiorstwa i know-how, https://tajemnica-przedsiebiorstwa.pl/dyrektywa-ue-tajemnica-przedsiebiorstwa-i-know-how/.
[12] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz.U. 1997 nr 133 poz. 883.
[13] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta; Art. 24. ust. 2; Dz.U. 2009 nr 52 poz. 417.
[14] Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej Dz.U. 2016 poz. 1579.
[15] Wytyczne w sprawie przejrzystości na mocy rozporządzenia 2016/679, Grupa Robocza Artykułu 29, https://gdpr.pl/wytyczne-grupy-roboczej-art-29-sprawie-przejrzystosci-mocy-rozporzadzenia-2016679.
[16] http://www.rodowzdrowiu.pl.
[17] https://gdpr.pl/wp-content/uploads/2018/06/Belgia_Zalecenie_w_sprawie_Rejestru_czynno%C5%9Bci_przetwarzania_danych.pdf.
[18] https://www.giodo.gov.pl/1520285.

Streszczenie

Celem niniejszego artykułu jest uporządkowanie i wprowadzenie pewnej systematyki do problemu bezpieczeństwa danych przetwarzanych w podmiotach leczniczych. Szum medialny, który był związany z wdrożeniem przepisów RODO, spowodował dużą nerwowość wszystkich

środowisk medycznych - nawet tych, które od lat poprawnie uregulowały w swoich podmiotach procedury bezpiecznego przetwarzania danych.

Nie można rozważać regulacji związanych z RODO bez uwzględnienia regulacji wprowadzającej jednolite narzędzia służące do bezpiecznego tworzenia dokumentów elektronicznych, dzięki powołaniu do życia w UE usług zaufania publicznego oraz identyfikacji wszystkich podmiotów uczestniczących w wymianie informacji w sieciach teleinformatycznych oraz uwierzytelnianiu serwerów.

Specyfika danych medycznych oraz systemu funkcjonowania instytucji opieki zdrowotnej stawia dodatkowe wyzwania przed systemami przetwarzającymi dane medyczne oraz powoduje brak jednolitego modelu systemu bezpieczeństwa.

Określone zostały podstawowe zasady przetwarzania danych osobowych, które muszą być zastosowane w odniesieniu do danych medycznych: Zasada zgodności z prawem, rzetelności i przejrzystości; zasada ograniczenia celu; zasada minimalizacji danych; zasada prawidłowości danych; zasada ograniczenia przechowywania; zasada integralności i poufności oraz zasada rozliczalności.

Obowiązująca obecnie w UE regulacja dotycząca ochrony danych różni się od dotychczas obowiązujących przepisów tym, że nie narzuca konkretnych rozwiązań wszystkim instytucjom i osobom przetwarzającym dane osobowe, zobowiązując podmioty do stworzenia swoich wewnętrznych modeli zapewniających ich bezpieczeństwo i poufność. W każdym podmiocie świadczącym usługi medyczne administrator danych - uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia - wdraża odpowiednie środki techniczne i organizacyjne.

Słowa kluczowe:

dane osobowe, dane wrażliwe, RODO, eIDAS, usługi zaufania publicznego, identyfikacja podmiotów