Rekomendacje
Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej

Warszawa, wrzesień 2017

Spis treści

Wprowadzenie

Niniejszy dokument stanowi rekomendację Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa informacji i ochrony danych osobowych oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej, a więc zawierającą zarówno elektroniczną dokumentację medyczną jak i pozostałą dokumentację medyczną niemieszczącą się w definicji elektronicznej dokumentacji medycznej.

Punktem wyjścia dla opracowania rekomendacji było przeanalizowanie sposobów przetwarzania danych, oraz samych danych wchodzących w skład dokumentacji medycznej przetwarzanej w postaci elektronicznej oraz wrażliwości poszczególnych ich grup. W opracowaniu odniesiono się do obecnej sytuacji formalnoprawnej, w oparciu o krajowe i europejskie przepisy ochrony danych osobowych oraz przepisy i regulacje branżowe.

Przeanalizowano także wymagania i zalecenia norm związanych z zapewnieniem bezpieczeństwa systemów informatycznych, co pozwala na określenie zaleceń dotyczących bezpiecznego przetwarzania dokumentacji medycznej w zależności od wybranego do jej przechowywania modelu architektury.

Wskazano również zagrożenia występujące podczas przetwarzania dokumentacji w postaci elektronicznej, a także przedstawiono praktyczny plan wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji jako podstawowego zabezpieczenia stosowanego przy przetwarzaniu danych osobowych.

Cel i przeznaczenie dokumentu

Celem niniejszego opracowania jest przedstawienie rekomendacji dla usługodawców w zakresie budowania i stosowania systemu bezpiecznego przetwarzania danych medycznych, dla podmiotów w których jest już przetwarzana dokumentacja medyczna w postaci elektronicznej, jak również dla podmiotów, które przygotowują się lub też wdrażają w swoich placówkach systemy informatyczne przetwarzające dokumentację medyczną w postaci elektronicznej. Opracowanie zawiera informacje w zakresie rozwiązań technicznych umożliwiających przetwarzanie dokumentacji medycznej w postaci elektronicznej. Na tej podstawie przedstawiono wymagania organizacyjne oraz wskazano odpowiedzialność za przetwarzanie informacji w tym danych osobowych wrażliwych zawartych w dokumentacji medycznej.

Dokument może mieć zastosowanie do wszystkich systemów przetwarzających dokumentację medyczną w postaci elektronicznej, zarówno systemów dedykowanych do przetwarzania Elektronicznej Dokumentacji Medycznej typu Rejestry i Repozytoria, a także do wszystkich systemów, w których przetwarzana jest dokumentacja medyczna, w tym do systemów szpitalnych i gabinetowych.

Niniejszy dokument skupia się na kwestii przetwarzania dokumentacji medycznej w podmiotach wykonujących działalność leczniczą lub przez podmioty działające w ich imieniu.

Rekomendacje uwzględniają konieczność przygotowania się podmiotów do wejścia w życie przepisów RODO i uwzględniają zarówno stan prawny obecny jak i stan prawny, który będzie obowiązywał od 25 maja 2018 roku, przy czym w związku z brakiem przepisów krajowych dostosowujących przepisy krajowe do wymogów RODO, CSIOZ deklaruje, że po wejściu ich w życie dokona aktualizacji - niniejszego dokumentu.

Ponadto wskazać należy, że w związku z art. 40 RODO, który zachęca do opracowywania przez organizacje branżowe kodeksów postępowania, administracja publiczna wraz z organizacjami branżowymi rozpoczęły współpracę nad opracowaniem ww. kodeksu dla podmiotów sektora ochrony zdrowia. Celem kodeksu jest doprecyzowanie zakresu zastosowania przepisów RODO. Poniższe Rekomendacje będą również uwzględnione podczas opracowywania postanowień kodeksu.

Rekomendacje mogą być także wykorzystywane przez dostawców, którzy podejmują się projektowania i budowy systemów informatycznych dedykowanych dla ochrony zdrowia.

Organizacja dokumentu

Nr rozdziału	Opis zawartości
Cześć I	Ogólne informacje dotyczące sposobów przetwarzania dokumentacji medycznej w postaci elektronicznej w aspekcie bezpieczeństwa informacji.
Część II	Dane podlegające przetwarzaniu w ramach przetwarzania dokumentacji medycznej w postaci elektronicznej oraz formalnoprawne zasady przetwarzania danych medycznych jako szczególnej kategorii danych osobowych
Część III	Zagrożenia i odpowiedzialność wynikająca z przetwarzania dokumentacji medycznej w postaci elektronicznej
Część IV	Zalecenia i rekomendacje dotyczące bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej

Tabela 1. Prezentacja zawartości opracowania

Podstawy prawne i organizacyjne

Podczas prac nad dokumentem wykorzystano następujące akty prawne i normy:

- Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2016 r. poz. 1535 z późn. zm.),

- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 z późn. zm.),
- Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. z 2016 r. poz. 1793, z późn. zm.),
- Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz.U. z 2016 r. poz. 1868, z późn. zm.),
- Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. z 2016 r. poz. 1638 z późn. zm.),
- Ustawa z dnia 6 września 2001 r. prawo farmaceutyczne (Dz.U. z 2016 r. poz. 2142),
- Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U z 2017 r. poz. 1318 z późn. zm.),
- Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. z 2017 r. poz. 125 z późn. zm.),
- Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz.U. z 2016 r. poz. 1866 z późn. zm.),
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922),
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r. poz. 1167),
- Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r. poz. 1579 z późn. zm.),
- Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2015 r. poz. 2069),
- Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2015 r. poz. 971 z późn. zm.),
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 113 z późn. zm.),
- Rozporządzenie Ministra Zdrowia z dnia 25 marca 2013 r. w sprawie klasyfikacji danych i systemu kodów w Systemie Informacji Medycznej (Dz.U. z 2013 r. poz. 473),

- Rozporządzenie Ministra Sprawiedliwości z dnia 26 lutego 2016 r. w sprawie rodzajów i zakresu dokumentacji medycznej prowadzonej w podmiotach leczniczych dla osób pozbawionych wolności oraz sposobu jej przetwarzania (Dz.U. z 2016 r. poz. 258),
- 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 Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. z 2006 r. Nr 206 poz. 1518),
- Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz.U. z 2016 r. poz. 1626),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 25 lutego 2016 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych (Dz.U. z 2016 r. poz. 249),
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U.UE.L.119.89),
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (Dz.U. UE.L.2016.194.1),
- 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 (Dz.U.UE.L.2014.257.73),
- 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) (Dz.U.UE.L.2016.119.1),
- Norma PN-EN 13609-1:2007 Informatyka w ochronie zdrowia -- Komunikaty do przechowywania informacji pomocniczych w systemach opieki zdrowotnej -- Część 1: Aktualizacja schematów kodowania,

- Norma PN-EN 13606-2:2009 Informatyka w ochronie zdrowia -- Przesyłanie elektronicznej dokumentacji zdrowotnej -- Część 2: Specyfikacja wymiany archetypów,
- Norma PN-EN 13606-3:2009 Informatyka w ochronie zdrowia -- Przesyłanie elektronicznej dokumentacji zdrowotnej -- Część 3: Archetypy referencyjne i listy terminów,
- Norma PN-EN 13606-4:2009 Informatyka w ochronie zdrowia - Przesyłanie elektronicznej dokumentacji zdrowotnej - Część 4: Bezpieczeństwo danych,
- Norma PN-EN ISO 13606-5:2010 - Informatyka w ochronie zdrowia -- Przesyłanie elektronicznej dokumentacji zdrowotnej -- Część 5: Specyfikacja interfejsu,
- Norma PN-ISO/IEC 27005:2014-01 Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji,
- ISO/IEC 27017:2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2014 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27033-1 — IT network security – Overview and concepts,
- ISO/IEC 27033-1:2015— Information technology - Security techniques - Network security - Part 1: Overview and concepts,
- ISO/IEC 27033-2:2012— Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security,
- ISO/IEC 27033-3:2010— Information technology - Security techniques - Network security - Part 3: Reference networking scenarios --Threats, design techniques and control issues,
- ISO/IEC 27033-4:2014— Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways - Risks, design techniques and control issues,
- ISO/IEC 27033-5:2013— Information technology - Security techniques - Network security - Part 5: Securing –communications across networks using Virtual Private Networks (VPNs) Risks, design techniques and control issues,
- ISO/IEC 27033-6:2016— Information technology - Security techniques - Network security - Part 6: IP network access,
- ISO/IEC 27033-7 — Information technology - Security techniques - Network security - Part 7: Wireless,

- PN-EN ISO/IEC 27001:2017-06 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania,
- PN-EN ISO 27799:2016-10 - Informatyka w ochronie zdrowia -- Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002,
- PN-EN ISO/IEC 27002:2017-06 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji,
- Norma PN-I-13335-1:1999 Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych,
- PN-EN ISO 10781:2015-11 Informatyka w ochronie zdrowia -- Model funkcjonalny systemu elektronicznej dokumentacji zdrowotnej HL7, wersja 2 (EHR FM),
- PN-EN ISO 21549-3:2014-05 - wersja angielska Informatyka w ochronie zdrowia -- Dane dotyczące karty zdrowia pacjenta -- Część 3: Ograniczony zestaw danych klinicznych.

Podczas prac nad opracowaniem dokumentu *„Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej”* wykorzystano poniższe publikacje i opracowania:

1. D. *Bogucka, Świętokrzyskie w awangardzie, Computerworld,* 27 września 2013 r.
2. *B. Borucki, Kardionet e-book. Ochrona poufności i bezpieczeństwa medycznych danych osobowych*, Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego Uniwersytet Warszawski.
3. *Dolnośląskie E-Zdrowie,* Biuletyn Informacyjny CSIOZ, Wydanie drugie, styczeń 2012 r.
4. *E-Zdrowie w województwie łódzkim*, Biuletyn Informacyjny CSIOZ, Wydanie pierwsze, listopad 2011 r.
5. *Kierunki rozwoju e-Usług w ochronie zdrowia w Województwie Zachodniopomorskim na lata 2011 – 2020*, Urząd Marszałkowski Województwa Zachodniopomorskiego, Szczecin, 28 czerwca 2011 r.
6. *Koncepcja architektury systemu informatycznego Podlaski System Informacyjny e-Zdrowie* - Załącznik nr 2 do dokumentu Opis Przedmiotu Zamówienia do przetargu nieograniczonego na wykonanie zamówienia publicznego: „Dostarczenie i wdrożenie zintegrowanego systemu informatycznego dla Projektu Podlaski System Informacyjny e-Zdrowie”, 8 kwietnia 2013 r.
7. *Koncepcja projektu technicznego Podlaski System Informacyjny e-Zdrowie* - Załącznik nr 3 do dokumentu Opis Przedmiotu Zamówienia do przetargu nieograniczonego na wykonanie zamówienia publicznego: „Dostarczenie i wdrożenie zintegrowanego systemu informatycznego dla Projektu Podlaski System Informacyjny e-Zdrowie”, 8 kwietnia 2013 r.
8. *Lubuska Sieć Teleradiologii – e-Zdrowie w diagnostyce obrazowej,* Biuletyn Informacyjny CSIOZ, Wydanie pierwsze, listopad 2011 r.

9. *Małopolski System Informacji Medycznej*, Biuletyn Informacyjny CISOZ, Wydanie dziewiąte, kwiecień 2013 r.
10. *Monitoring strategii rozwoju Województwa Mazowieckiego do roku 2020. Raport*, Samorząd Województwa Mazowieckiego, Warszawa, marzec 2011 r.
11. K. Nyczaj, *Informatyzacja ochrony zdrowia*, Służba Zdrowia, nr 17-24 z 14 marca 2013 r.
12. K.Nyczaj, *Informatyzacja ochrony zdrowia*, „Służba Zdrowia" nr 60-68 z 29 sierpnia 2011 r.
13. K. Nyczaj, *Jak bezpiecznie archiwizować elektroniczną dokumentację medyczną*, Serwis Kadry Zarządzającej ZOZ nr 23, październik 2011.
14. K. Nyczaj, *Kiedy dopuszczalne jest przetwarzanie danych medycznych poza siedzibą świadczeniodawcy*, Serwis Kadry Zarządzającej ZOZ nr 22, wrzesień 2011.
15. K. Nyczaj, *Outsourcing elektronicznej dokumentacji medycznej*, Służba Zdrowia nr 43-50 (40444051), 13 czerwca 2011 r.
16. K. Nyczaj, P. Piecuch, *Elektroniczna dokumentacja medyczna,* Wydawnictwo Wiedza i Praktyka sp. z o.o., Warszawa 2013 r.
17. K. Nyczaj, P. Piecuch, *Technologie i IT w medycynie. W co warto inwestować?,* Wydawnictwo Wiedza i Praktyka sp. z o.o., Warszawa 2012 r.
18. *Opis Przedmiotu Zamówienia PSIM w postępowaniu o udzielenie zamówienia publicznego na dostawę pod nazwą: „Budowa i wdrożenie Podkarpackiego Systemu Informacji Medycznej"* – Załącznik nr 1 do SIWZ, 15 marca 2013 r.
19. *Opracowanie rekomendacji klasyfikacji elektronicznej dokumentacji medycznej,* Infovide Matrix, doradca strategiczny CSIOZ, czerwiec 2012 r.
20. *Podlaski System Informacyjny e-Zdrowie – gdzie jesteśmy i dokąd zmierzamy w 2013 roku*, Biuletyn Informacyjny CSIOZ, Wydanie ósme, luty 2013 r.
21. *Praktyczne aspekty wdrożenia Elektronicznej Dokumentacji Medycznej w Medicover Sp. z o.o.,* Biuletyn Informacyjny CSIOZ, Wydanie szóste, wrzesień 2012 r.
22. *Raport Cloud computing: elastyczność, efektywność, bezpieczeństwo*, Microsoft, Instytut Badań nad Gospodarką Rynkową, 2011 r.
23. *Regionalny Program Strategiczny w zakresie ochrony zdrowia Zdrowie dla Pomorzan - Załącznik nr 1 do Uchwały nr 930/274/13 Zarządu Województwa Pomorskiego z dnia 8 sierpnia 2013 r.*, Zarząd Województwa Pomorskiego, Gdańsk 2013 r.
24. *Specyfikacja Istotnych Warunków Zamówienia AD V 333/56/2009: Usługa polegająca na opracowaniu koncepcji i studium wykonalności projektu „e-Usługi-eOrganizacja - pakiet rozwiązań informatycznych dla jednostek organizacyjnych województwa kujawsko-pomorskiego" realizowana w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2007-2013* – Załącznik nr 3 Szczegółowy opis przedmiotu zamówienia, 29 maja 2009 r.
25. *Specyfikacja Istotnych warunków Zamówienia (SIWZ) Małopolskiego Systemu Informacji Medycznej* – Załącznik nr 7 i 8 do SIWZ, 28 czerwca 2010 r.
26. *Specyfikacja Istotnych warunków Zamówienia (SIWZ): Modernizacja istniejących oraz wdrożenie nowych systemów informatycznych w zakładach opieki zdrowotnej podległych*

Samorządowi Województwa Łódzkiego w ramach projektu "Usługi Regionalnego Systemu Informacji Medycznej (RSIM-Usługi)"- Załącznik nr 1.1 do SIWZ, 20 sierpnia 2012 r.

27. *Strategia Rozwoju Województwa Mazowieckiego do roku 2020 (aktualizacja),* Samorząd Województwa Mazowieckiego, wydanie I, Warszawa 2006 r.
28. *Studium Wykonalności dla projektu „Podkarpacki System Informacji Medycznej",* Centrum Rozwoju Społeczno-Ekonomicznego, Sielec, listopad 2010 r.
29. *Studium Wykonalności projektu inwestycyjnego pt.: „Dolnośląskie E-Zdrowie",* Wrocław, czerwiec 2009 r.
30. *Więcej za mniej. Trendy IT 2012,* Praca zbiorowa pod red. R. Jesionka, 2011 r. 31. ww.telepom.eu/pl
31. *Opinia 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej (WP 196), Grupa Robocza art. 29, 2012 r.*
32. *Ochrona danych medycznych według najnowszych przepisów 25 praktycznych porad,* Praca zbiorowa pod redakcją Mariusza Jendry, Wiedza i Praktyka, 2015r.
33. *Opinia 2/2015 w sprawie kodeksu postępowania dotyczącego przetwarzania danych w chmurze opracowanego przez grupę roboczą C-SIG (Cloud Select Industry Group) (WP232), Grupa Robocza art. 29, 2015 r.*
34. *Elektroniczna dokumentacja medyczna. Wdrożenie i prowadzenie w placówce medycznej. Aktualne przepisy na 2017 rok, Krzysztof Nyczaj, Paweł Piecuch, Wiedza i Praktyka, 2016 r.*
35. *Ochrona danych medycznych i osobowych pacjentów,* Praca zbiorowa pod redakcją Mariusza Jendry, Wiedza i Praktyka, 2017 r.
36. *Bezpieczeństwo danych w chmurze: Dane przesyłane są do USA? Nie wiadomo,* Tomasz Jurczak, Gazeta Prawna.Pl, 2015 r.
37. *Ochrona danych osobowych medycznych.* C.H. Beck, Praca zbiorowa dr inż. Kajetan Wojsyk, dr Paweł Litwiński, Mariusz Jagielski, Monika Krasińska, Piotr Kawczyński, 2016 r.
38. *Krajowe ramy interoperacyjności. Systemy informatyczne w administracji publicznej.* C.H. Beck, A. Gałach, 2015 r.
39. *Ochrona danych osobowych w dziale I, IT Professional, Praca zbiorowa Andrzej Boboli, Mateusz Borkiewicz, Kamil Koszewicz, Grzegorz Leśniewski, Wrocław 2017.*
40. *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych.* C.H. Beck, Praca zbiorowa pod red. Macieja Kołodzieja. 2017 r.
41. *https://www.zdrowie.abc.com.pl/artykuly/pacjent-nie-ma-prawa-do-usuniecia-danych-osobowych-ktore-posiada-placowka,15984.html ; Iwona Kaczorowska-Kossowska. 2015r.*
42. *https://www.gazeta-msp.pl/?id=pokaz_artykul&indeks_artykulu=1084&nr_historyczny=87; Michał Koralewski. 2009r.*
43. *https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/ochrona-danych-osobowych/newsletter-rodo0/administrator-danych-musi-umiec-wykazac-ze-dziala-zgodnie-z-prawem.html*

Słownik skrótów i pojęć

Poniższe tabele przedstawiają definicje skrótów i pojęć w układzie alfabetycznym, które zostały użyte w dokumencie.

Lp.	Skrót lub pojęcie	Definicja
1.	**Certyfikat uwierzytelniający**	Certyfikat elektroniczny generowany przez zewnętrznego dostawcę lub podmiot przetwarzający dokumentację medyczną, w celu uwierzytelniania pracowników placówki medycznej w dostępie do danych medycznych
2.	**Cloud computing in. chmura obliczeniowa**	Zgodnie z definicją podawaną przez amerykański Narodowy Instytut Standaryzacji i Technologii (NIST) jest to model umożliwiający powszechny, wygodny, udzielany na żądanie dostęp za pośrednictwem sieci do wspólnej puli możliwych do konfiguracji zasobów przetwarzania (np. sieci, serwerów, przestrzeni przechowywania, aplikacji i usług), które można szybko dostarczyć i uwolnić przy minimalnym wysiłku zarządzania lub działań dostawcy usług
3.	**DICOM**	Obrazowanie Cyfrowe i Wymiana Obrazów w Medycynie (ang. Digital Imaging and Communications in Medicine) źródło: http://medical.nema.org/
4.	**DokMedR**	Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015 poz. 2069)
5.	**DokPrzetwR**	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 r. Nr 100 poz. 1024)
6.	**Dyrektywa 95/46/WE**	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
7.	**Elektroniczna Dokumentacja Medyczna - EDM**	Zgodnie z art. 2 pkt 6 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U. z 2016 r. poz. 1535 z późn. zm.): Elektroniczna dokumentacja medyczna – dokumenty wytworzone w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym Profilem Zaufanym: a) umożliwiające usługobiorcy uzyskanie od usługodawcy świadczenia opieki zdrowotnej określonego rodzaju, z wyłączeniem zleceń na wyroby medyczne, b) określone w przepisach wydanych na podstawie art. 13a;
8.	**eWUŚ**	Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców

9.	**Grupa Robocza art. 29**	Grupa Robocza art. 29 ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołaną na mocy art. 29 Dyrektywy 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 jako niezależny podmiot o charakterze doradczym
10.	**Hosting**	Usługa polegająca na udostępnianiu przez dostawcę usług internetowych zasobów serwerowni między innymi takich jak określonej objętości dysku twardego, maksymalnej ilości danych do przesłania przez łącza internetowe serwerowni i maksymalnej mocy obliczeniowej
11.	**HSM**	ang. *Hardware Security Module*, urządzenie do przechowywania i zarządzania kluczami bezpieczeństwa do autoryzacji i przetwarzania kryptograficznego.
12.	**IaaS**	ang. *Infrastructure as a Service* – rodzaj chmury obliczeniowej typu Infrastruktura jako usługa - usługa umożliwiająca użytkownikowi zapewnienie przetwarzania, przechowywania, sieci lub innych zasadniczych zasobów przetwarzania, w której użytkownik może uruchomić i stosować dowolne oprogramowanie, które może obejmować systemy operacyjne i aplikacje. Użytkownik nie zarządza źródłową infrastrukturą chmury i nie kontroluje jej, lecz ma kontrolę nad systemami operacyjnymi, przechowywaniem i uruchomionymi aplikacjami; a także możliwie ograniczoną kontrolę nad wybranymi elementami sieci (np. firewallem gospodarza)
13.	**Kolokacja**	Usługa polegająca na przekazaniu firmie zewnętrznej serwerów lub innych urządzeń teleinformatycznych do dedykowanych do tego celu pomieszczeń zwanych serwerowniami
14.	**Outsourcing**	Przedsięwzięcie polegające na wydzieleniu ze struktury organizacyjnej przedsiębiorstwa realizowanych przez nie funkcji i przekazaniu ich do realizacji innym podmiotom gospodarczym
15.	**PaaS**	ang. *Platform as a Service* – rodzaj chmury obliczeniowej typu Platforma jako usługa - usługa umożliwiająca użytkownikowi uruchomienie w infrastrukturze chmury stworzonych przez siebie lub zakupionych aplikacji stworzonych z wykorzystaniem języka i narzędzi programowania wspieranych przez dostawcę. Użytkownik nie zarządza źródłową infrastrukturą chmury i nie kontroluje jej, w tym sieci, serwerów, systemów operacyjnych lub przestrzeni przechowywania, lecz ma kontrolę nad uruchomionymi aplikacjami i ewentualnie nad konfiguracją środowiska hostingu aplikacji
16.	**RODO**	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)
17.	**SaaS**	ang. *Software as a Service* – rodzaj chmury obliczeniowej typu Oprogramowanie jako usługa - usługa umożliwiająca użytkownikowi korzystanie z aplikacji dostawcy działających w infrastrukturze chmury. Aplikacje są dostępne z różnych urządzeń klienta za pomocą interfejsu, na przykład przeglądarki internetowej (np. poczta elektroniczna na stronie

		internetowej). Użytkownik nie zarządza źródłową infrastrukturą chmury i nie kontroluje jej, w tym sieci, serwerów, systemów operacyjnych, przestrzeni przechowywania, a nawet poszczególnych funkcji aplikacji, z ewentualnym wyjątkiem ograniczonych ustawień konfiguracji aplikacji przez danego użytkownika
18.	**SLA**	ang. *Service Level Agreement* – umowa utrzymania i systematycznego poprawiania ustalonego między klientem a usługodawcą poziomu jakości usług poprzez stały cykl obejmujący: uzgodnienia, monitorowanie usługi, raportowanie, przegląd osiąganych wyników
19.	**System informatyczny**	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
20.	**Szyfrowanie**	proces zamiany tekstu jawnego w szyfrogram (inaczej kryptogram) w taki sposób że ich odczytanie jest możliwe tylko przez upoważnione osoby.
21.	**TLS**	ang. *Transport Layer Security* – rozwinięcie protokołu SSL, zapewnia poufność i integralność przesyłanych danych, może również służyć do uwierzytelnienie serwera oraz klienta
22.	**UODO**	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. 2016 poz. 922)
23.	**UPrPacjRPP**	Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta t.j. (Dz.U. z 2017 r. poz. 1318 z późn. zm)
24.	**USIOZ**	Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U. z 2016 r. poz. 1535 z późn. zm.)
25.	**XML**	ang. *Extensible Markup Language* – uniwersalny język formalny (niezależny od platformy) przeznaczony do reprezentowania danych w sposób strukturalizowany

Tabela 2. Słownik skrótów i pojęć

Poniższa tabela przedstawia zawarte w RODO definicje skrótów i pojęć, które użyte zostały w dokumencie.

Lp.	Skrót lub pojęcie	Definicja
1.	**administrator**	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania
2.	**dane osobowe**	oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na

		podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej
3.	**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
4.	**dane genetyczne**	oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej
5.	**dane biometryczne**	oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne
6.	**naruszenie ochrony danych osobowych**	oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
7.	**odbiorca**	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane 4.5.2016 L 119/33 Dziennik Urzędowy Unii Europejskiej PL osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania
8.	**podmiot przetwarzający**	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora
9.	**przetwarzanie**	oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie
10.	**profilowanie**	oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się

11.	**pseudonimizacja**	oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
12.	**strona trzecia**	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe
13.	**zbiór danych**	oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie
14.	**zgoda**	osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

Tabela 3. Definicje zawarte w RODO

Część I. Ogólne informacje dotyczące sposobów przetwarzania dokumentacji medycznej w postaci elektronicznej w aspekcie bezpieczeństwa informacji

1. Modele architektury bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej

W niniejszym rozdziale zaprezentowane zostały modele architektury przetwarzania dokumentacji medycznej w postaci elektronicznej przez usługodawców. Przedstawiono klasyczny model przetwarzania danych, modele wykorzystywane w ramach korzystania z możliwości outsourcingu (kolokacja, hosting) oraz chmury obliczeniowej. Zaprezentowano również koncepcje platform regionalnych o zasięgu wojewódzkim tworzone dla usługodawców działających w danym regionie administracyjnym.

Decydując się na wybór jednego z opisanych poniżej modeli przetwarzania danych usługodawca określa podział i poziom odpowiedzialności za przetwarzanie danych oraz za wykorzystywane zasoby IT pomiędzy sobą, a podmiotem zewnętrznym.

Poniższa tabela przedstawia podział kontroli i odpowiedzialności pomiędzy usługodawcą a podmiotem zewnętrznym w poszczególnych modelach przetwarzania dokumentacji medycznej.

	Model klasyczny	**Kolokacja**	**Hosting**
Serwer	Usługodawca	Usługodawca	Podmiot zewn.
Sieć	Usługodawca	Podmiot zewn.	Podmiot zewn.
Środowisko wykonywalne*	Usługodawca	Usługodawca	Usługodawca
Aplikacja	Usługodawca	Usługodawca	Usługodawca
Dane	Usługodawca	Usługodawca	Usługodawca

Tabela 4. Podział kontroli i odpowiedzialności pomiędzy usługodawcą, a podmiotem zewnętrznym w poszczególnych modelach przechowywania elektronicznej dokumentacji medycznej

*Środowisko wykonywalne wskazane w powyższej tabeli rozumiane jest jako zestaw oprogramowania umożliwiającego uruchomienie aplikacji do prowadzenia dokumentacji medycznej w postaci elektronicznej po stronie serwerowej. W zależności od technologii wykonania aplikacji mogą to być:

- system operacyjny serwera, na którym jest uruchomiona aplikacja,
- oprogramowanie serwera aplikacyjnego oraz serwera WWW,
- oprogramowanie umożliwiające wirtualizację infrastruktury serwerowej, na której uruchamiana jest aplikacja.

W skład środowiska wykonywalnego nie wchodzi oprogramowanie klienckie oraz oprogramowanie pośredniczące, wykorzystywane jako interfejs dostępowy do aplikacji przetwarzających dokumentację medyczną (np. przeglądarka internetowa, system operacyjny stacji końcowej użytkownika). Za wskazane elementy w każdym z modeli odpowiedzialny jest usługodawca.

W modelu klasycznym usługodawca posiada niemal pełną kontrolę nad posiadaną infrastrukturą i oprogramowaniem. Jednak w wielu wypadkach jego samowystarczalność jest ograniczona koniecznością korzystania z usług dostawców łączy internetowych.

W modelu kolokacji usługodawca przekazuje firmie zewnętrznej serwery lub inne urządzenia teleinformatyczne do przeznaczonych do tego celu pomieszczeń (serwerowni). Podmiot zewnętrzny odpowiada również za zapewnienie odpowiedniego łącza.

W modelu hostingu usługodawca dzierżawi od podmiotu zewnętrznego serwer lub część jego przestrzeni dyskowej.

W modelu chmury obliczeniowej typu IaaS infrastruktura informatyczna jest wynajmowana od podmiotu zewnętrznego. Usługodawca zachowuje kontrolę nad danymi i oprogramowaniem.

W modelu chmury obliczeniowej typu PaaS zwiększa się zakres kontroli podmiotu zewnętrznego, który dostarcza środowisko, w którym usługodawca może instalować aplikacje i zarządzać nimi.

Najmniejszy zakres kontroli usługodawca posiada w modelu chmury obliczeniowej typu SaaS. Zachowuje on jedynie kontrolę nad danymi. Całość infrastruktury wraz z oprogramowaniem pozostają pod kontrolą podmiotu zewnętrznego, który odpowiada za ich bezawaryjne działanie.

Systemy usługodawców mogą być dostępne w trybie 24h/7 dni w tygodniu lub innym, zależnie od specyfiki usługodawcy. Dla wybranego trybu dostępności należy zapewnić odpowiedni poziom usług świadczonych przez podmioty zewnętrzne realizujące usługi asysty na sprzęt i oprogramowanie w formie wymagań SLA określonych w umowach z tymi podmiotami.

Poniżej opisano szczegółowo poszczególne modele.

1.1 Model klasyczny

W modelu klasycznym usługodawca posiada własną infrastrukturę informatyczną i w związku z tym ponosi koszt zakupu serwerów, infrastruktury sieciowej, oprogramowania, zapewnienia

pomieszczenia odpowiednio przygotowanego do pracy serwera, zapewnienia zespołu zajmującego się konserwacją sprzętu, usuwaniem awarii.

Niezależnie od architektury technicznej oraz logicznej rozwiązania, w modelu klasycznym całość odpowiedzialności za bezpieczeństwo danych i zapewnienie ciągłości działania usług leży po stronie usługodawcy (właściciela systemu informatycznego). Szczegółowy opis zawierający minimalne wymagania i zalecenia dotyczące bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej dla modelu klasycznego przedstawiony został w załączniku nr 1 do niniejszego opracowania.

Ważne

W modelu klasycznym usługodawca posiada niemal pełną kontrolę nad posiadaną infrastrukturą i oprogramowaniem. Jednak w wielu wypadkach jego samowystarczalność jest ograniczona koniecznością korzystania z usług dostawców łączy internetowych.

1.2 Outsourcing

Outsourcing to przedsięwzięcie polegające na wydzieleniu ze struktury organizacyjnej przedsiębiorstwa realizowanych przez nie funkcji i przekazaniu ich do realizacji innym podmiotom często gospodarczym.

Przy wyborze tego modelu należy przeanalizować ryzyko większego uzależnienia od dostawcy zewnętrznego niż w przypadku modelu klasycznego.

Uwarunkowania prawne w zakresie możliwości wykorzystania modelu outsourcingu omówiono w części II rekomendacji.

Kolokacja

Kolokacja to usługa polegająca na przekazaniu firmie zewnętrznej serwerów lub innych urządzeń teleinformatycznych do dedykowanych do tego celu pomieszczeń - serwerowni.

Serwerownia to pomieszczenie przygotowane w sposób zapewniający jak najbardziej efektywne działanie serwerów. Zapewnia ono optymalne warunki klimatyczne (temperaturę, wilgotność), bezpieczeństwo danych (ochronę fizyczną, sprzętową, zabezpieczenia przeciwpożarowe, monitoring, podtrzymanie zasilania w przypadku awarii prądu, redundancja łącz, tak by w przypadku awarii obciążenie przejęło łącze zapasowe) oraz szybkie łącza. W przypadku przesyłania i pobierania dużej ilości danych z serwera szczególnie istotne jest zapewnienie łącza o wysokiej przepustowości wysyłania i pobierania danych tzw. łącz dedykowanych. W tym przypadku serwer jest formalnie własnością usługodawcy, zaś outsourcing polega na powierzeniu zarządzania nim w specjalistycznym ośrodku przetwarzania danych.

Szczegółowy opis zawierający minimalne wymagania i zalecenia dotyczące bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej dla modelu kolokacji przedstawiony został w załączniku nr 2 do niniejszego opracowania.

Ważne

W modelu kolokacji usługodawca przekazuje firmie zewnętrznej serwery lub inne urządzenia teleinformatyczne do przeznaczonych do tego celu pomieszczeń (serwerowni). Podmiot zewnętrzny odpowiada również za zapewnienie odpowiedniego łącza.

Hosting (serwer dedykowany, serwer VPS):

a. **Serwer dedykowany**
b. **Serwer VPS** (wirtualny serwer prywatny/ wirtualny serwer dedykowany)

Rozwiązania opierające się o hosting budzą zwykle najmniej wątpliwości prawnych, ponieważ usługodawca zachowuje prawo do miejsca, gdzie przetwarzane są dane medyczne jego pacjentów. Tym niemniej kwestia korzystania z usług innych podmiotów w celu przetwarzania przez nich dokumentacji medycznej w postaci elektronicznej musi zostać przeanalizowana w każdym przewidywanym modelu (scenariuszu) indywidualnie przez usługodawców wdrażających takie rozwiązania.

Serwer dedykowany to oddzielny komputer o określonych zasobach sprzętowych przeznaczony dla danego usługodawcy. Może zostać skonfigurowany wg potrzeb usługodawcy i wykorzystywanego przez niego oprogramowania. Jest to rozwiązanie wygodne, jednak kosztowne, co może stanowić barierę jego wykorzystania dla części jednostek medycznych.

Serwer VPS (wirtualny serwer prywatny/ wirtualny serwer dedykowany) to rozwiązanie stanowiące alternatywę dla rozwiązania opartego o serwer dedykowany. Polega ono na dzierżawie części przestrzeni dyskowej serwera o gwarantowanych parametrach (tj. ilość pamięci RAM, pojemność dysku, dostęp do procesora). Wirtualizacja polega na logicznym podziale serwera na kilka mniejszych serwerów wirtualnych zachowujących funkcjonalność serwera dedykowanego. Przydzielone zasoby sprzętowe nie są współdzielone z innymi użytkownikami, co zapewnia ochronę przed spowolnieniem czy też przerwaniem pracy. Jest to rozwiązanie korzystne dla mniejszych jednostek (np. indywidualnych praktyk lekarskich, pielęgniarskich i położnych), które nie mają możliwości zakupienia własnego serwera lub nie mają miejsca na magazynowanie sprzętu. W przypadku serwera VPS usługodawca płaci tylko za faktycznie wykorzystane zasoby, które określane są po wykonaniu analizy potrzeb. Zaletą tego rozwiązania są znacznie niższe niż w przypadku serwera dedykowanego koszty przy zapewnieniu analogicznej funkcjonalności. Szczegółowy opis zawierający minimalne wymagania

i zalecenia dotyczące bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej dla modelu hostingu przedstawiony został w załączniku nr 3 do niniejszego opracowania.

Ważne

W modelu hostingu usługodawca dzierżawi od podmiotu zewnętrznego serwer lub określoną objętość dysku twardego, maksymalną ilość danych do przesłania przez łącza internetowe serwerowni i maksymalną mocy obliczeniową.

1.3 Cloud computing (chmura obliczeniowa)

W tym podrozdziale wyjaśniono pojęcie chmury obliczeniowej oraz przedstawiono opis występujących na rynku rozwiązań. Uwarunkowania prawne określające możliwość korzystania z chmur obliczeniowych oraz wymagania co do ich stosowania omówiono w części II rekomendacji - zasady przetwarzania danych osobowych w szczególności danych medycznych.

Cloud computing czyli przetwarzanie danych w chmurze obliczeniowej to obecnie jedna z najszybciej rozwijających się usług informatycznych. Wprowadza ona nowy model zarządzania zasobami IT, w którym firmy nie ponoszą nakładów na własną infrastrukturę informatyczną, lecz korzystają z wynajętej infrastruktury lub aplikacji za pośrednictwem sieci. W modelu tym komputery stają się wyłącznie terminalami do prezentacji wyników operacji przeprowadzanych przez centra przetwarzania danych.

Przetwarzanie danych ma charakter mierzalny (np. liczba przesłanych bajtów, czas korzystania), dlatego odbiorca ponosi koszty tej usługi w zależności od faktycznego wykorzystania zasobów.

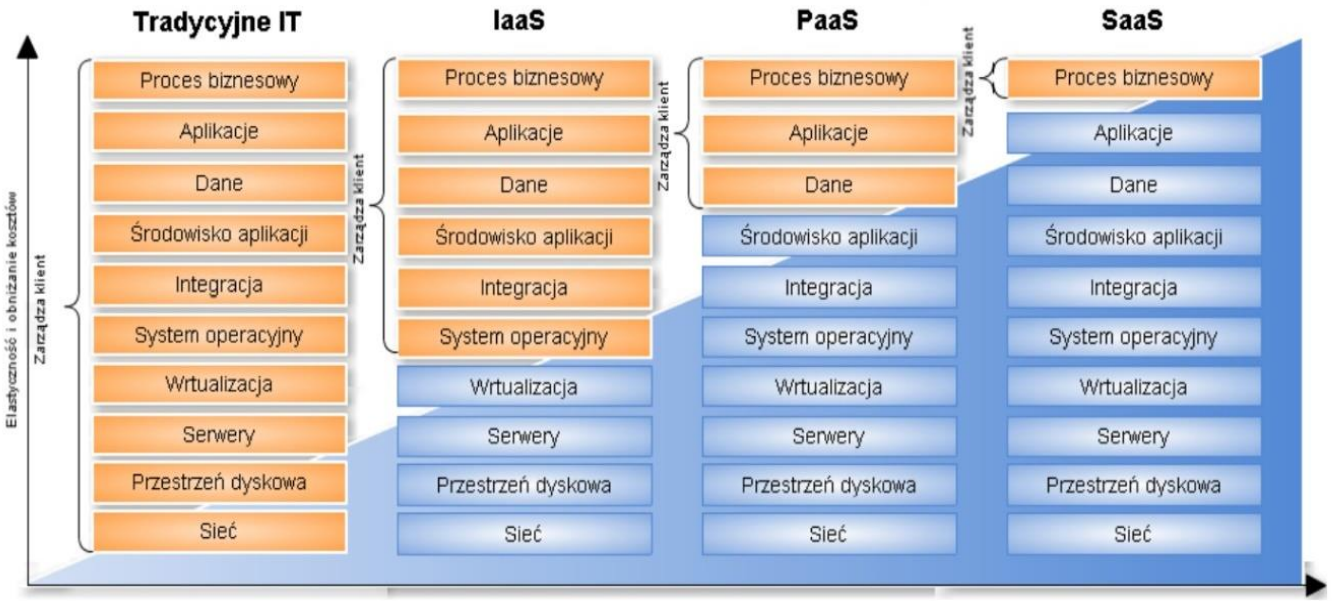
Chmurę stanowi więc cały zbiór serwerów, oprogramowania, sieci itd., do którego dostęp uzyskuje się za pośrednictwem Internetu.

Opis istniejących rozwiązań

W zależności od stopnia złożoności dostarczanych usług rozróżnia się następujące rodzaje cloud computingu:

- Infrastructure as a Service – IaaS (Infrastruktura jako usługa),
- Platform as a Service – PaaS (Platforma jako usługa),
- Software as a Service – SaaS (Oprogramowanie jako usługa).

Poniższy rysunek przedstawia podział kontroli pomiędzy usługodawcą a podmiotem zewnętrznym w poszczególnych modelach przetwarzania danych z zastosowaniem rozwiązań chmury obliczeniowej.



Rys.1. Podział kontroli pomiędzy usługodawcą a podmiotem zewnętrznym w modelach przetwarzania danych w chmurze obliczeniowej

Infrastructure as a Service – IaaS (Infrastruktura jako usługa) to usługa polegająca na korzystaniu ze sprzętu informatycznego za pośrednictwem Internetu. Może mieć ona np. formę korzystania z przestrzeni na wirtualnym dysku przeznaczonej do przechowywania danych, miejsca na serwerze wydzierżawionym w celu instalacji własnego systemu operacyjnego, czy też mocy obliczeniowej serwerów. W ramach tej usługi odbiorca instaluje samodzielnie potrzebne systemy operacyjne, komponenty i aplikacje. Dzięki temu, unika kosztownych inwestycji w sprzęt, a koncentruje się na warstwie aplikacyjnej. Odbiorca ma ogromne możliwości konfiguracji, musi jednak samodzielnie zadbać o zapewnienie bezpieczeństwa danych. W tym modelu dane przechowywane są w konkretnym miejscu i przetwarzane za pomocą dostarczanej infrastruktury.

Szczegółowy opis zawierający minimalne wymagania i zalecenia dotyczące bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej dla chmury obliczeniowej IaaS przedstawiony został w załączniku nr 3 do niniejszego opracowania.

Platform as a Service – PaaS (Platforma jako usługa) to usługa, w ramach której odbiorca uzyskuje dostęp nie tylko do infrastruktury, ale również do środowiska (w tym platformy programistycznej) rozumianego jako narzędzie do instalowania, uruchamiania i rozwijania aplikacji. Rozwiązanie to oferuje środowisko deweloperskie umożliwiające tworzenie i rozwijanie oprogramowania. Odbiorca nie ma dostępu do systemu operacyjnego, na którym jest uruchomiona platforma, ani do przestrzeni dyskowej, na której są składowane dane. Dostęp możliwy jest tylko do samej platformy, co jest dalej idącym ograniczeniem niż w przypadku modelu IaaS. Usługa ta jest zazwyczaj wykorzystywana przez odbiorców w celu rozwijania i hostingu prawnie chronionych rozwiązań opartych o aplikacje w celu spełnienia wewnętrznych wymogów lub świadczenia usług stronom trzecim.

Szczegółowy opis zawierający minimalne wymagania i zalecenia dotyczące bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej dla chmury obliczeniowej PaaS przedstawiony został w załączniku nr 4 do niniejszego opracowania.

Ważne

W modelu chmury obliczeniowej typu PaaS zwiększa się zakres kontroli podmiotu zewnętrznego, który dostarcza środowisko, w którym usługodawca może zarządzać zainstalowanymi aplikacjami.

Software as a Service – SaaS (Oprogramowanie jako usługa) to usługa, w ramach której odbiorca uzyskuje dostęp nie tylko do infrastruktury sprzętowej wraz ze środowiskiem operacyjnym, ale również do określonych aplikacji. W odróżnieniu od modelu PaaS wykorzystywane oprogramowanie jest własnością dostawcy, dlatego też odpowiada on za jego aktualizację i niezawodność. Restrykcje odnośnie dostępu są w tym modelu największe, ponieważ odbiorca nie posiada kontroli nad platformą niezbędną do działania aplikacji, systemem operacyjnym niezbędnym do działania platformy i przestrzenią dyskową służącą do zapisu danych z aplikacji.

Szczegółowy opis zawierający minimalne wymagania i zalecenia dotyczące bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej dla chmury obliczeniowej SaaS przedstawiony został w załączniku nr 5 do niniejszego opracowania.

Ważne

W model chmury obliczeniowej typu SaaS usługodawca ma najmniejszy zakres kontroli. Zachowuje on jedynie kontrolę nad danymi. Całość infrastruktury wraz z oprogramowaniem pozostaje pod kontrolą podmiotu zewnętrznego, który odpowiada za ich bezawaryjne działanie.

Ważne

IaaS, PaaS czy SaaS jest to model rozwiązania, który może być oparty zarówno na chmurze publicznej jak i prywatnej.

Chmura prywatna a chmura publiczna (cloud computing)

W zależności od stopnia kontroli zasobów informatycznych udostępnianych w formie usługi rozróżnia się następujące rodzaje cloud computingu:

- public cloud computing (publiczna chmura obliczeniowa),
- private cloud computing (prywatna chmura obliczeniowa).

W przypadku chmury publicznej korzysta się ze współdzielonej infrastruktury udostępnianej przez podmioty zewnętrzne za pośrednictwem Internetu. Podstawową cechą chmury publicznej jest jej ogólnodostępny charakter. Podmiot oferujący usługę w ramach chmury publicznej umożliwia dostęp dla wielu odbiorców na tych samych warunkach, zachowując bezpieczeństwo świadczenia usług. Odbiorcy tej usługi korzystają w całości z zewnętrznych zasobów informatycznych - właścicielem całej infrastruktury jest zewnętrzny dostawca i to on odpowiada za zapewnienie odpowiedniej przestrzeni dla danych, ich bezpieczeństwo i bezawaryjne działanie. Dane przetwarzane są w infrastrukturze rozproszonej, często na serwerach w różnych częściach świata. W tym przypadku zarówno system jak i dane znajdują się poza placówką medyczną.

Możliwe jest również korzystanie za pośrednictwem chmury publicznej z usług podmiotów, które nie są dostawcą chmury. Przykładowo, gdy użytkownik chce skorzystać z aplikacji, której dostawca chmury nie ma w swojej ofercie, możliwe jest zainstalowanie takiego oprogramowania w środowisku operacyjnym udostępnionym w chmurze.

W przypadku tego rozwiązania szczególne znaczenie ma szybkość i niezawodność łącza internetowego w placówce medycznej, ponieważ w przypadku zerwania połączenia nie posiada ona dostępu do danych i możliwości korzystania z systemu. Zapewnienie łącza o odpowiednio dużej przepustowości ma podstawowe znaczenie w przypadku przesyłania plików o dużych rozmiarach np. z diagnostyki obrazowej.

Chmura prywatna jest projektowana dla danej organizacji. W tym przypadku infrastruktura informatyczna jest dedykowana na potrzeby określonej organizacji i jest wyłączona ze współdzielenia z innymi podmiotami. Infrastruktura ta może być zlokalizowana w siedzibie organizacji lub poza nią (przykładowo serwery mogą być kolokowane, tj. mogą znajdować się w serwerowni w podmiocie zewnętrznym, lub ze względów bezpieczeństwa mogą być rozlokowane w kilku miejscach).

Organizacja może wykorzystywać własną infrastrukturę (jeśli organizacja posiada własną serwerownię lub centrum przetwarzania danych, może umożliwić dostęp do danych i aplikacji za pomocą przeglądarki w obrębie własnej sieci, bez konieczności instalowania aplikacji na stanowiskach) lub też korzystać z możliwości hostowania chmury prywatnej u zewnętrznego dostawcy np. w dużym data center. W przypadku własnej infrastruktury wymagany jest zakup specjalnego oprogramowania, które połączy wewnętrzne zasoby sprzętowe w jedną pulę, która będzie mogła być dynamicznie przydzielana w zależności od faktycznego zapotrzebowania ze strony użytkowników.

Zarządzanie infrastrukturą może odbywać się przy pomocy wewnętrznych służb IT lub być powierzone podmiotowi zewnętrznemu.

W odróżnieniu od chmur publicznych czy hybrydowych stanowiących połączenie chmury publicznej i prywatnej, chmury prywatne są używane przez jedną organizację, a przechowywane dane są całkowicie odizolowane. Wszelkie dane i usługi udostępniane są więc w ramach jednej organizacji. W tym modelu placówka medyczna przechowuje i przetwarza dane na dedykowanych dla niej serwerach.

Pełne wdrożenie tego rozwiązania zakłada, że wszystkie dane oraz zasoby wykorzystywane przez pracowników placówki medycznej są przechowywane na centralnych serwerach sieciowych. Umożliwia to dostęp do danych z dowolnego terminala, stacji roboczej na terenie placówki medycznej, jak również dostęp przy pomocy urządzeń mobilnych (np. smartfona, tabletu).

Ważną zaletą chmury prywatnej jest bezpieczeństwo danych i brak rewolucyjnych zmian w momencie jej wprowadzania. Po przeniesieniu danych do chmury zmianie ulega tylko sposób korzystania ze wsparcia działu IT, który po zbudowaniu chmury udostępnia aplikacje w postaci usługi, do których użytkownicy uzyskują dostęp przy pomocy urządzeń dostępowych (terminali, stacji roboczych, urządzeń mobilnych).

NIST określił cechy, które powinny posiadać zarówno rozwiązania chmury publicznej jak i prywatnej:

- **Samoobsługa** – odbiorca usługi powinien mieć możliwość samodzielnego, automatycznego zamówienia i otrzymania zasobów niezbędnych do przetwarzania danych (np. moc obliczeniowa, pamięć, dostęp do bazy danych, dostęp do aplikacji). Uzyskanie dostępu do nowych zasobów nie powinno wymagać ingerencji ze strony dostawcy.
- **Dostęp z każdego miejsca** – dostęp do zasobów jest realizowany przez łącze szerokopasmowe. Rozwiązania udostępniane w chmurze powinny być dostępne za pomocą standardowych narzędzi jak np. przeglądarka internetowa z każdego miejsca (jeśli jest to wymagalne) na różnych urządzeniach (takich jak smartfony, tablety, laptopy, komputery stacjonarne) oraz na innych urządzeniach dostępnych obecnie oraz w przyszłości.
- **Współdzielenie zasobów** – użytkownicy chmury powinni korzystać ze współdzielonej puli zasobów (zasoby takie jak moc obliczeniowa, pamięć, sieć, dysk powinny być przydzielane użytkownikom ze współdzielonej puli). Technologią, która umożliwia łączenie niejednolitych zasobów w pulę jest wirtualizacja. Pula jest współużytkowana na zasadzie dynamicznego przydziału i zwalniania precyzyjnie określonych porcji zasobów wirtualnych. Użytkownicy nie muszą być świadomi fizycznej lokalizacji tych zasobów.

- **Elastyczność i skalowalność** – należy zapewnić możliwość szybkiego zastrzegania i uwalniania zasobów w zależności od zapotrzebowania na usługi. Powinno odbywać się to automatycznie. Dzięki temu możliwe jest dynamiczne skalowanie rozwiązania w zależności od popytu na usługę.
- **Mierzalność usług** – dostawcy usług prowadzą ciągły monitoring i pomiar wykorzystania zasobów. Z jednej strony umożliwia to dokonywanie optymalizacji pracy posiadanych zasobów, z drugiej zaś umożliwia rozliczanie z odbiorcą usług w oparciu o faktyczne wykorzystanie zasobów.

Można wyróżnić także wspomnianą wcześniej tzw. chmurę hybrydową, stanowiącą rozwiązanie mieszane.

Chmura hybrydowa to rozwiązanie polegające na ulokowaniu części zasobów w chmurze prywatnej a części w chmurze publicznej. W praktyce część serwerów może znajdować się wewnątrz jednostki i służyć do przechowywania danych, natomiast same usługi mogą być udostępniane zdalnie z serwerów należących do podmiotu zewnętrznego. Można również przyjąć inne rozwiązanie, w ramach którego w chmurze prywatnej przetwarzane są dane strategiczne lub prawnie chronione, a w chmurze publicznej są przetwarzane dane mniej istotne.

Możliwości wykorzystania publicznej chmury obliczeniowej, wiążą się z wieloma ograniczeniami, ponieważ przetwarzanie danych odbywa się na serwerach wirtualnych w środowisku współdzielonym. Usługodawca nie ma do czynienia z odrębną jednostką (komputerem), ale z wydzielonym logicznie środowiskiem, w którym otrzymuje określoną liczbę serwerów, przestrzeń dyskową, moc obliczeniową. Przydzielanie zasobów (np. przestrzeni dyskowej) odbywa się w tym przypadku dynamicznie na wielu równocześnie funkcjonujących komputerach, w związku z czym nie da się wskazać konkretnego miejsca przechowywania danych. W rozdziale II szeroko wskazano warunki, jakie muszą zostać spełnione, aby można było efektywnie i bezpiecznie wykorzystać dostępne na rynku rozwiązania chmurowe.

W każdym jednak przypadku mając na uwadze uwarunkowania prawne dotyczące zastosowania zabezpieczeń adekwatnych do poziomu przetwarzanych informacji w zakresie rozwiązań chmurowych należy je rozpatrywać indywidualnie.

Dostępne są rozwiązania chmurowe, które dzięki zastosowaniu odpowiedniej technologii kryptograficznej uniemożliwiają dostęp dostawcy rozwiązań do danych należących do organizacji i przechowywanych w chmurze. Technologie takie wykorzystują zaawansowane metody ochrony prywatnych kluczy szyfrujących, które są dzielone i nigdy nie są przetrzymywane w całości w jednym miejscu. W takiej sytuacji serwer nie jest w stanie uzyskać dostępu do danych w postaci jawnej (serwer nie posiada, ani nie może wyznaczyć żadnego z kluczy kryptograficznych klienta usługi), treść danych pozostaje tajemnicą nawet dla dostawcy usługi.

Ważne

W przypadku rozwiązań chmurowych dostęp do danych możliwy jest dla dostawcy rozwiązań. Dlatego zalecane jest stosowanie mechanizmów kryptograficznych w celu zabezpieczenia przed udostępnieniem danych osobom nieupoważnionym oraz zapewnienia pełnej poufności danych.

Biorąc pod uwagę bezpieczeństwo przetwarzania danych w chmurze obliczeniowej należy podkreślić, że najłatwiej jest zabezpieczyć chmurę prywatną, ponieważ do ochrony własnej serwerowni wystarczą tradycyjne systemy zabezpieczania danych. W przypadku chmury publicznej dostawca oferuje największy zakres zabezpieczeń dla chmury typu SaaS. Dostawca odpowiada wówczas za sprzęt, system operacyjny i aplikacje. Użytkownik otrzymuje większy zakres zabezpieczeń, jednak traci możliwość kontroli konfiguracji środowiska. W przypadku chmury typu IaaS użytkownik otrzymuje od dostawcy jedynie sprzęt (maszyny wirtualne), zaś system operacyjny i aplikacje pozostają pod kontrolą użytkownika. W tym przypadku to na użytkowniku spoczywa odpowiedzialność za zapewnienie bezpieczeństwa. W takiej sytuacji brak odpowiedniej wiedzy i umiejętności oraz właściwych systemów zabezpieczeń opartych na technologiach kryptograficznych, może doprowadzić do wycieku danych.

Ważne

W przypadku wyboru rozwiązań opartych o przetwarzanie danych medycznych w chmurze obliczeniowej, należy brać pod uwagę zalecenia wynikające z opinii Grupy Roboczej art.29, GIODO jak również wytycznych zawartych w obowiązujących normach.

Standardowe umowy z dostawcami rozwiązań w chmurze nie zawierają szczegółowych zapisów dotyczących bezpieczeństwa. Umowy te są dostosowane do usługi, a nie do konkretnego klienta. Z powodu masowego charakteru usług, ich elastyczność jest niewielka. W umowie z dostawcą usługi przetwarzania danych w chmurze powinna znajdować się klauzula audytu umożliwiająca sprawdzenie dostawcy pod względem wymagań bezpieczeństwa.

W celu zagwarantowania odpowiedniego poziomu bezpieczeństwa oraz świadczonych usług zalecane jest korzystanie z atestowanych centrów danych. Obecnie stosowanymi standardami związanymi z certyfikacją usług w chmurze są: standard SAS70 wydawany przez Amerykański Instytut Biegłych Rewidentów AICPA (American Institute of Certified Public Accountants), w USA zastępowany standardem SSAE16 oraz standard ISAE 3000 wydawany przez IAASB (The International Auditing and Assurance Standards Board). Należy jednak zwrócić uwagę na fakt, że zakres ISAE3402 obejmuje zabezpieczenia dotyczące raportowania finansowego, co może nie być do końca zbieżne z wymaganiami dla ochrony danych osobowych. Niektórzy dostawcy oferują również rozwiązania chmurowe posiadające certyfikat ISO/IEC 27018 dotyczący ochrony danych osobowych w chmurze.

Dostawca usługi (w zależności od przyjętego modelu) powinien również zapewnić, że dane w procesie przekazywania i przechowywania w chmurze obliczeniowej są szyfrowane, a wykorzystane rozwiązania zapewniają ochronę danych w modelu end-to-end encryption.

Ponadto dostawca usługi chmury obliczeniowej dostarczający technologię transmisji danych powinien zapewnić, że z uwagi na dużą liczbę możliwych podatności nie stosuje on standardowych protokołów transmisji tj. SSL/TLS - powinny być stosowane mechanizmy uniemożliwiające skuteczne prowadzenie podsłuchu transmisji czy też ataki typu man in the middle.

Dodatkowo dostawca usługi powinien przekazać pełną informację dotyczącą podwykonawców i podmiotów współpracujących, mających udział w dostarczaniu usługi chmury obliczeniowej. Każdy z podwykonawców powinien być traktowany również jako przetwarzający dane osobowe i być związany takimi samymi klauzulami umownymi jak dostawca usługi. Odbiorca usługi powinien pozostać wyłącznym administratorem danych osobowych przekazanych do chmury. Dostawca usługi powinien również poinformować odbiorcę usługi o wszelkich zobowiązaniach publicznych wobec organów ścigania, służb specjalnych w zakresie przekazywania i dostępu do danych zamieszczanych w chmurze obliczeniowej.

Decydując się na wykorzystanie rozwiązania opartego o model chmury obliczeniowej zaleca się również wzięcie pod uwagę standardów wypracowywanych przez organizację Cloud Security Alliance (CSA), stawiającą sobie za cel promowanie najlepszych praktyk w zakresie bezpieczeństwa chmur obliczeniowych. Organizacja ta opracowała przewodnik *„Security guidance for critical areas of focus in cloud computing”* mający na celu dostarczenie zbioru najlepszych praktyk dla menadżerów i użytkowników, którzy chcą korzystać z usług przetwarzania w chmurze w bezpieczny sposób .

Organizacja ta opracowała również Cloud Control Matrix (CCM) - macierz wymagań z zakresu bezpieczeństwa dla dostawców i odbiorców usług w chmurze. Macierz ta została zbudowana w oparciu o wymagania powszechnie uznawanych standardów, norm, regulacji i najlepszych praktyk, takich jak ISO 27001/27002, ISACA COBIT, PCI DSS, NIST, HIPAA / HITECH i Jericho Forum. Może ona stanowić narzędzie wspomagania odbiorców usług w chmurze w ocenie i analizie ryzyka związanego z tym modelem.

Ważne

Usługodawca powinien dokonać analizy prawnej wykorzystania danego modelu z uwzględnieniem wszystkich indywidualnych okoliczności wdrożenia.

Decydując się na wybór określonego modelu przetwarzania danych usługodawca określa podział odpowiedzialności pomiędzy siebie a podmiot zewnętrzny, nad wykorzystywanymi zasobami IT w zakresie zapewnienia bezpieczeństwa. Im więcej obowiązków zostanie powierzonych, tym mniejszą będzie miał usługodawca odpowiedzialność, ale jednocześnie mniejszą kontrolę.

1.4 Przetwarzanie dokumentacji medycznej w postaci elektronicznej na przykładzie platform regionalnych

Aktualnie działa, bądź w najbliższym czasie zacznie działać 8 platform regionalnych o zasięgu wojewódzkim - platformy: podkarpacka, podlaska, świętokrzyska, łódzka, wielkopolska, dolnośląska, małopolska oraz mazowiecka. W obecnej perspektywie finansowej województwa planują rozbudowę już działających platform regionalnych, jak również budowę i wdrożenie kolejnych. W ramach platform, w zależności od regionu, funkcjonuje od kilku do kilkudziesięciu podmiotów leczniczych. Działające obecnie platformy opierają się na dwóch głównych modelach: klasycznym oraz outsourcingu - w zależności od przyjętego sposobu przechowywania dokumentacji medycznej - oraz na modelu mieszanym.

Niezależnie od wybranego rozwiązania podmioty biorące udział w projekcie (budowie platformy regionalnej) podpisały ze sobą umowy, w ramach których regulowane są kwestie przechowywania, przetwarzania i wymiany elektronicznej dokumentacji medycznej oraz danych osobowych, a także odpowiedzialności i obowiązków partnerów za realizację oraz przyznawanie uprawnień do Systemu.

Podmioty wykonujące działalność leczniczą na podstawie podpisanych porozumień lub umów zgodnie z obowiązującymi przepisami prawa mogą pomiędzy Systemami Informatycznymi przekazywać EDM pacjenta, na potrzeby aktualnie obsługiwanych zdarzeń medycznych. Przekazywanie lub dostęp do EDM dla uprawnionych podmiotów lub personelu medycznego odbywa się na wniosek pacjenta lub w przewidzianych prawem przypadkach.

Kluczowe znaczenie ma w tym przypadku proces wymiany EDM w ramach systemów informatycznych powstałych lub powstających w ramach platform regionalnych.

W ramach wymiany EDM za pośrednictwem platform można zidentyfikować następujące modele wymiany danych:

1. **Model rozproszony** – wymiana EDM pomiędzy podmiotami - każdy z każdym. Pacjent leczony w jednym podmiocie wyraża zgodę na pobranie wskazanego przez niego zakresu EDM z odbytego wcześniej pobytu w innym podmiocie wykonującym działalność leczniczą.
   W modelu rozproszonym na platformie regionalnej znajduje się indeks EDM umożliwiający określenie miejsca/miejsc składowania EDM pacjenta, natomiast EDM znajduje się w lokalnych repozytoriach EDM w podmiotach.
2. **Model z regionalnym repozytorium EDM** – podmioty w ramach podpisanych porozumień oraz wydanych przez pacjentów zgód przekazują EDM do regionalnego repozytorium.
   Pacjent przebywając w podmiocie wyraża zgodę na pobranie lub udostępnienie wskazanego przez niego zakresu EDM podmiotowi lub personelowi medycznemu realizującemu obsługę danego zdarzenia medycznego. Do zadań regionalnego repozytorium EDM należy: utrzymywanie i udostępnianie indeksu EDM, przechowywanie informacji o zgodach pacjenta na udostępnianie dokumentów, zarządzanie informacją o udostępnieniu EDM.

3. **Model mieszany** – łączący model rozproszony z modelem regionalnego repozytorium, gdzie EDM dotycząca części dokumentacji medycznej jest dostępna w repozytorium regionalnym (np. dane opisowe obrazowych badań diagnostycznym), a pozostała część dokumentacji (np. dane obrazowe w formacie DICOM) znajduje się w lokalnym repozytorium EDM zlokalizowanym w podmiocie (w miejscu gdzie EDM została wytworzona).

W modelu z regionalnym repozytorium EDM, platforma oprócz procesu udostępniania najczęściej zapewnia funkcjonalność backup-u EDM dla poszczególnych podmiotów współtworzących platformę regionalną, a w przypadku małych podmiotów platformę hostingową umożliwiającą tworzenie EDM.

Innym rodzajem procesu wymiany EDM pomiędzy podmiotami jest wykonywanie usług medycznych w ramach podpisanych umów na podwykonawstwo. Przykładem tego może być zlecanie i wykonywanie badań obrazowych lub laboratoryjnych u podwykonawców (podstawą prawną z reguły jest podpisana umowa na świadczenie usług).

Część II. Dane podlegające przetwarzaniu w ramach przetwarzania dokumentacji medycznej w postaci elektronicznej oraz formalnoprawne zasady przetwarzania danych medycznych jako szczególnej kategorii danych osobowych

1. Dane podlegające przetwarzaniu w ramach przetwarzania dokumentacji medycznej w postaci elektronicznej

Rekomendacje R (97) 5 Komitetu Ministrów Rady Europy wyznaczyły europejskie standardy w zakresie interpretacji „danych medycznych". W polskim tłumaczeniu tych rekomendacji „dane medyczne" zostały przetłumaczone jako „dane dotyczące zdrowia". Rekomendacje wskazują, że sformułowanie *„dane dotyczące zdrowia"* oznacza wszelkie dane osobowe dotyczące stanu zdrowia tej osoby. Wyrażenie odnosi się również do danych mających oczywisty i ścisły związek ze zdrowiem oraz z danymi genetycznymi. Oznacza to, że dane medyczne to kategoria danych osobowych, która powinna podlegać szczególnej ochronie. Wskazać należy, iż treść rekomendacji jest zgodna ze stanowiskiem przedstawionym w dyrektywie 95/46/WE. Dyrektywa tak jak rekomendacja, traktuje dane dotyczące zdrowia jako dane osobowe i podobnie jak rekomendacja zapewnia im szczególną ochroną, uznając ich wrażliwy charakter.[1]

Zgodnie z oficjalnym komentarzem do Rekomendacji[2] pojęcie danych medycznych obejmuje dane odnoszące się do przeszłego, obecnego i przyszłego stanu zdrowia podmiotu danych, zarówno zdrowia fizycznego, jak i psychicznego. Ponadto pojęcie to odnosi się do wszelkich informacji, które nie są informacjami upublicznionymi, a które pozwalają na ustalenie szeroko pojętego stanu zdrowia jednostki, takich jak styl życia osoby, życie seksualne czy nałogi.

Przepisy UODO należy traktować jako realizację wymagań zawartych w dyrektywie 05/46/WE i jednocześnie jako akceptację rekomendacji R (97) 5.[3]

Zgodnie z art. 27 ust. 1 UODO[i] dane o stanie zdrowia zaliczane są do katalogu danych wrażliwych. W katalogu danych wrażliwych wymienione zostały dane ujawniające 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.

RODO w dużym stopniu powtarza wypracowane i przyjęte stanowiska z ww. dokumentów. Jednocześnie RODO rozwija koncepcje danych o stanie zdrowia. Zgodnie z art. 4 pkt 15 RODO *„dane*

[1] Ochrona danych osobowych medycznych. C.H. Beck, Praca zbiorowa dr inż. K. Wojsyk, dr P. Litwiński, .M. Jagielski, M. Krasińska, P. Kawczyński, 2016 r.
[2] Rekomendacja R (97) 5 Komitetu Ministrów do Państw Członkowskich
[3] Tamże.

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 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.*

RODO wprowadza wspólną precyzyjną i jednolicie interpretowaną terminologię danych o stanie zdrowia.

Ważne

Pojęcie danych medycznych jest bardzo szerokie i nie ma wątpliwości, że dokumentacja medyczna jest dokumentacją zawierającą dane osobowe wrażliwe tj. dane o stanie zdrowia a zatem podlega ochronie na poziomie wysokim. Wytyczne zawarte w niniejszym dokumencie winny być stosowane do dokumentacji medycznej jako całości.

Od 25 maja 2018 r. dane wrażliwe zostaną rozszerzone o nową kategorię danych, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej (art. 9 ust 1[ii] RODO).

Należy pamiętać, że wymienione powyżej typy danych należy traktować nierozłącznie, a zatem przykładowo dane o życiu seksualnym czy nałogach mogą być jednocześnie danymi o stanie zdrowia.

UODO[4] zabrania przetwarzania danych wrażliwych poza kilkoma wyjątkowymi sytuacjami, do których należy między innymi przetwarzanie prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych.

Pojęcie danych medycznych jest bardzo szerokie i nie ma wątpliwości, że dokumentacja medyczna jest dokumentacją zawierającą dane osobowe wrażliwe tj. dane o stanie zdrowia podlega więc ochronie na poziomie wysokim.

[4] Art. 27 - Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 poz. 922.)

Zgodnie z art. 2 pkt 6 USIOZ przez elektroniczną dokumentację medyczną należy rozumieć dokumenty wytworzone w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym Profilem Zaufanym:

a) umożliwiające usługobiorcy uzyskanie od usługodawcy świadczenia opieki zdrowotnej określonego rodzaju, z wyłączeniem zleceń na wyroby medyczne,

b) określone w przepisach wydanych na podstawie art. 13a.

Jednocześnie w art. 2 pkt. 7 USIOZ zdefiniowano czym są jednostkowe dane medyczne :

- jednostkowe dane medyczne – dane osobowe oraz inne dane osób fizycznych dotyczące uprawnień do udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej, stanu zdrowia, a także inne dane przetwarzane w związku z planowanymi, udzielanymi i udzielonymi świadczeniami opieki zdrowotnej oraz profilaktyką zdrowotną i realizacją programów zdrowotnych.

Dokumentacja medyczna w postaci elektronicznej to każdy dokument elektroniczny umożliwiający usługobiorcy uzyskanie świadczenia opieki zdrowotnej określonego rodzaju oraz dokumentacja wytworzona w postaci elektronicznej, zawierająca dane o udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej. Dokumentacja taka zawierać będzie jednostkowe dane medyczne, które zgodnie z USIOZ określone są jako dane osobowe oraz inne dane osób fizycznych dotyczące uprawnień do udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej, stanu zdrowia, a także inne dane przetwarzane w związku z planowanymi, udzielanymi i udzielonymi świadczeniami opieki zdrowotnej oraz profilaktyką zdrowotną i realizacją programów zdrowotnych jak również zdarzenia medyczne przetwarzane w systemie informacji - czynności w ramach świadczenia zdrowotnego lub świadczenia zdrowotnego rzeczowego, o których mowa w ustawie z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, której dane są przetwarzane w systemie informacji.

Przetwarzanie takich danych zobowiązuje administratorów danych osobowych jakimi są kierownicy poszczególnych placówek medycznych do zapewnienia należytego ich zabezpieczenia i zapewnienia przetwarzania zgodnie z przepisami prawa.

Zapewnienie bezpieczeństwa i poufności informacji o stanie zdrowia pacjentów to jeden z priorytetów przetwarzania takich informacji, pacjenci bowiem dostarczają osobom sprawującym nad nimi opiekę bardzo osobiste informacje, których ujawnienie mogłoby wpłynąć negatywnie chociażby na osobiste relacje społeczne czy też utrudnić korzystanie z wielu usług.

Należy również mieć na uwadze, że zgodnie z art. 51 ust. 1 UODO *Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2*. Natomiast zgodnie z art. 82 ust. 2 RODO każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym ochronę danych osobowych

W związku z koniecznością zapewnienia bezpiecznego przetwarzania danych osobowych w systemie, który przetwarza dokumentację medyczną, istotne jest również posiadanie świadomości wrażliwości poszczególnych danych.

Ważne

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Zgodnie z *rozporządzeniem Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu, i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (2015r. poz. 2069),* prowadzenie dokumentacji w systemie teleinformatycznym powinno się odbywać m.in. z zapewnieniem stałego dostępu do dokumentacji dla osób uprawnionych oraz zabezpieczeniem przed dostępem osób nieuprawnionych.

W celu poprawnego określenia zakresu dostępu do danych w systemie powinny zostać w nim zidentyfikowane role jakie mogą istnieć wraz ze wskazaniem poziomu dostępu do danych osobowych.

W systemie dla usługodawców medycznych można wyróżnić następujące przykładowe role, które będą przetwarzać dane związane z dokumentacją medyczną w placówce ochrony zdrowia:

- Pacjent
- Osoby upoważnione przez Pacjenta
- Lekarz / Lekarz dentysta / Felczer,
- Pielęgniarka / położna - rola ograniczona do działań wyłącznie medycznych,
- Pielęgniarka / położna - rola rozszerzona o działania pomocnicze,
- Pracownik ratownictwa medycznego,
- Pracownik medyczny,
- Personel administracyjny,
- Farmaceuta,
- Diagnosta laboratoryjny,
- Technik farmacji,
- Realizator zleceń,
- Administrator usługodawcy.

W celu określenia profili uprawnień do danych należy wziąć pod uwagę wrażliwość poszczególnych danych osobowych oraz zakres informacji do jakich powinien mieć dostęp użytkownik systemu otrzymujący uprawnienia wynikające z profilu do którego został przypisany.

1.1. Pozostałe dane niebędące dokumentacją medyczną

Poza przechowywaniem w systemach informatycznych danych medycznych może zajść potrzeba przechowywania informacji dodatkowych związanych ze świadczeniem usług medycznych. Przykładem takich informacji może być komunikat wysyłany do systemu eWUŚ oraz odpowiedź zwrotna z tego systemu. Potrzeba przechowywania komunikatów w systemach usługodawców może wynikać z chęci posiadania informacji o dotychczas wysyłanych zapytaniach do systemu eWUŚ zarówno w celach statystycznych czy też funkcjonalnych systemu np. wysyłanie zapytania tylko raz danego dnia.

Komunikat taki może zawierać dane osobowe jak PESEL, imię, nazwisko w związku z tym dane takie powinny być również odpowiednio chronione i zabezpieczone przed dostępem osób nieuprawnionych np. w przypadku przechowywania takich informacji w systemie usługodawcy.

2. Formalnoprawne zasady przetwarzania danych osobowych w szczególności danych medycznych

Obowiązek zabezpieczenia danych medycznych nakładają na usługodawcę w szczególności przepisy dotyczące ochrony danych osobowych, przepisy branżowe i inne regulacje:

1. UODO;
2. RODO;
3. rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI), wydane na podstawie art. 18 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. Dla podmiotów tych jest to dokument obligatoryjny natomiast dla podmiotów prywatnych będzie to dokument pomocniczy;

Dodatkowo pomocniczymi dokumentami będą dokumenty:

1. grupa norm serii 20000, 27000, 24762, 31000, 32000;
2. wytyczne przedstawione przez Grupę Roboczą art. 29 oraz pojawiające się krajowe i europejskie interpretacje przepisów ochrony danych osobowych

2.1 Formalnoprawne uwarunkowania ochrony danych osobowych

Przepisy dotyczące ochrony danych osobowych nakładają na podmioty przetwarzające dane osobowe w tym dane wrażliwe jakimi są dane medyczne, liczne obowiązki, które należy uwzględnić podczas projektowania systemów informatycznych.

Przepisy RODO opisują zasady oraz prawa osób, których dane dotyczą.

Art. 5 ust. 1[iii] RODO wskazuje na sześć zasad przetwarzania danych osobowych:

1. **Zasada zgodności z prawem**, **rzetelności i przejrzystości przetwarzania** – wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem, rzetelne i przetwarzane w sposób zrozumiały dla osoby, której dane dotyczą. Jest to podstawowa zasada określająca relacje pomiędzy podmiotem danych i ich administratorem. Oznacza ona, że podmiot przetwarzający dane zawsze i na każdym etapie przetwarzania danych jest zobowiązany dbać o interesy osoby, której dane dotyczą. Musi spełniać co najmniej jeden z przewidzianych prawem warunków dopuszczalności przetwarzania danych (np. osoba, której dane dotyczą, wyrazi na to zgodę, przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych). Jednocześnie musi dołożyć staranności w zabezpieczeniu interesów osoby której przetwarzane dane dotyczą (zapewnić bezpieczeństwo danych między innymi poprzez ich pseudonimizację i szyfrowanie) oraz zagwarantować tej osobie kontrolę nad procesem przetwarzania (przekazywanie informacji do których ma prawo umożliwiających podejmowanie decyzji, między innymi: kto jest administratorem danych, w jaki celu i zakresie dane są zbierane i przetwarzane, jakie jest źródło danych, w jaki sposób są udostępniane itd.).[5]
2. **Zasada ograniczoności celu** - dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1[iv] RODO za niezgodne z pierwotnymi celami. Oznacza to, że administrator jest związany celem ustalonym na początku procesu przetwarzania i nie może go dowolnie zmieniać. Przepisy prawa zezwalają jednak wykorzystywać dane do celów archiwalnych i w interesie publicznym, do celów badań naukowych lub historycznych oraz do celów statystycznych, jednak pod warunkiem, że działania te są zgodne z ustalonymi w tym zakresie wymaganiami.[6]
3. **Zasada minimalizacji danych** – przetwarzane dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Nie wolno zbierać i przetwarzać danych, które nie są niezbędne do osiągnięcia celu przetwarzania i są w stosunku do niego nadmiarowe (np. zbieranie informacji o stanie zdrowia

[5] Ochrona danych osobowych medycznych. C.H. Beck, Praca zbiorowa dr inż. K. Wojsyk, dr P. Litwiński, .M. Jagielski, M. Krasińska, P. Kawczyński, 2016 r.
[6] Tamże

od pracowników, zbieranie informacji o wyznaniu od pacjenta, zbieranie wraz z danymi niezbędnymi do świadczenia usług medycznych informacji o adresie e-mail do celów marketingowych).[7]

4. **Zasada prawidłowości** – przetwarzane dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Obowiązkiem administratora jest dbałość o to, aby dane były prawidłowe i aktualizowane oraz zapewnienie, że dane które są nieprawidłowe względem celów przetwarzania zostaną niezwłocznie usunięte lub sprostowane.[8]
5. **Zasada ograniczoności przechowywania** - dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1^{v} RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy rozporządzenia RODO w celu ochrony praw i wolności osób, których dane dotyczą.
6. **Zasada integralności i poufności** – dotyczy stosowania odpowiednich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzanych danych osobowych. Między innymi chodzi o ochronę przed niedozwolonym przetwarzaniem lub przetwarzaniem niezgodnym z prawem a także zabezpieczenie danych przez ich utratą, zniszczeniem lub uszkodzeniem.

Ważne

RODO określa sześć zasad dotyczących przetwarzania danych - zasadę zgodności z prawem, rzetelności i przejrzystości przetwarzania, zasadę ograniczoności celu, zasadę minimalizacji danych, zasadę prawidłowości, zasadę ograniczoności przechowywania oraz zasadę integralności i poufności. Zasady te znajdują uszczegółowienie w konkretnych przepisach dotyczących przetwarzania.

Przepisy o ochronie danych osobowych zapewniają osobom, których dane dotyczą, szczególne prawa. Zgodnie z przepisami prawa osoba, której dane dotyczą ma prawo:

1. **Prawo do informacji i dostępu do danych**- Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Obejmuje to prawo dostęp osób, których dane dotyczą, do danych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi. Dlatego też każda

[7] Tamże.
[8] Tamże.

osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania. Administrator powinien móc udzielić zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji. Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie. Aktualnie zakres obowiązku informacyjnego w związku ze zbieraniem danych określa art. 25[vi] oraz art. 26[vii] UODO a także art. 32 ust 1 pkt 1-5a oraz ust. 5[viii] UODO w zakresie informacji na żądanie.

Od 25 maja 2018 r. będą to odpowiednio art. 13, 14 i 15[ix] RODO.

Ścisły związek z tym prawem mają przepisy § 7[x] DokPrzetwR. Administrator powinien zwrócić szczególną uwagę aby system informatyczny w którym dane będą przetwarzane zapewniał zgodność z tym przepisem tj. dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten musi zapewniać odnotowanie:

- daty pierwszego wprowadzenia danych do systemu;
- identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
- źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
- informacji o odbiorcach, w rozumieniu art. 7 pkt 6[xi] UODO, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
- sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8[xii] UODO.

Odnotowanie informacji, o których mowa w pkt 1 i 2, musi następować automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system musi zapewniać sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa powyżej.

W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa powyżej w pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

Od dnia 25 maja 2018 r. w zakresie realizacji prawa do informacji i dostępu do danych oraz jego zakresu i sposobu zbierania i przechowywania kierować się będziemy art. 15 RODO. Zgodnie z przedmiotowym przepisem, osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

a) cele przetwarzania;
b) kategorie odnośnych danych osobowych;
c) odbiorcy lub kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu -np przepis prawa lub czas trwania kampanii marketingowej;
e) prawo do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
h) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz przynajmniej w tych przypadkach istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

Prawo do uzyskania kopii, o której mowa powyżej (art. 15 ust. 3 RODO), nie może niekorzystnie wpływać na prawa i wolności innych.

2. **Prawo do poprawienia danych** – prawo to zwane także prawem do sprostowania polega na tym, że osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego uzupełnienia dotyczących jej danych osobowych, które są niekompletne, uaktualnienia danych jeżeli są nieaktualne oraz sprostowania danych jeżeli są one nieprawdziwe, w tym poprzez przedstawienie dodatkowego oświadczenia. Prawo do poprawienia danych jest obecnie uregulowane w art. 32 ust. 1 pkt 6[xiii] oraz art. 35[xiv] UODO.
   Zgodnie z art. 32 ust. 1 pkt 6 UODO każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych a zwłaszcza prawo do żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego

wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

Zgodnie z art. 35 ust. 1 UODO warunkiem skorzystania z prawa, o którym wyżej mowa jest wykazanie przez zainteresowanego, że dane są niepełne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy bądź są już niepotrzebne do realizacji celu, dla którego były gromadzone. Zgodnie z w/w przepisem UODO administrator powinien uwzględnić żądania bez zbędnej zwłoki, chyba że żądanie dotyczy danych, których tryb uzupełnienia, uaktualnienia lub sprostowania regulują odrębne ustawy. W sytuacji gdy administrator nie uwzględni żądania osoby, której dane dotyczą, to ma ona możliwość wystąpienia do Generalnego Inspektora Ochrony Danych Osobowych z wnioskiem o nakazanie dopełnienia tego obowiązku. Jak wynika z art 35 ust. 3 ustawy administrator danych ma obowiązek poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych o uaktualnieniu bądź sprostowaniu danych.

Od 25 maja 2018 r. osoba, której dane dotyczą będzie mogła skorzystać z prawa do poprawienia danych na zasadach określonych w art. 16[xv] oraz art. 19[xvi] RODO. Na podstawie art. 16 RODO będzie ona mogła żądać od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, będzie miała prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. Zgodnie z art. 19 RODO administrator będzie zobowiązany do informowania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 lub art. 18 RODO każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

3. **Prawo do żądania usunięcia danych** – zwane także prawem do bycia zapomnianym.
   Zgodnie z UODO osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania w przypadku jeżeli jej dane przetwarzane są na potrzeby marketingu

bezpośredniego w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim;

d) dane osobowe były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego tj. w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

Aktualnie obowiązujące przepisy w tym zakresie to art. 7 pkt 5[xvii], art. 32 ust. 1 pkt 6[xviii]-8 i ust 2-3[xix] oraz art. 35[xx] UODO.

Od 25 maja 2018 r. zastosowanie będą miały przepisy RODO zawarte w art. 17 -19[xxi] RODO.

Aby wzmocnić prawo do „bycia zapomnianym" w Internecie, twórcy RODO rozszerzyli prawo do usunięcia danych poprzez zobowiązanie administratora, który upublicznił te dane osobowe, do poinformowania administratorów, którzy przetwarzają takie dane osobowe o usunięciu wszelkich łączy do tych danych, kopii tych danych osobowych lub ich replikacji. Spełniając ten obowiązek administrator powinien podjąć racjonalne działania z uwzględnieniem dostępnych mu technologii i środków, w tym dostępnych środków technicznych, w celu poinformowania administratorów, którzy przetwarzają dane osobowe, o żądaniu osoby, której dane dotyczą.

Jeżeli administrator upublicznił dane osobowe, a na mocy art. 17 ust. 1 RODO ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

Przepisy art. 17 ust. 1 i 2 RODO nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;
b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 RODO;
d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
e) do ustalenia, dochodzenia lub obrony roszczeń.

Podobnie jak w przypadku prawa do poprawienia danych tak i w przypadku prawa do żądania usunięcia danych administrator informuje o usunięciu danych osobowych lub ograniczeniu przetwarzania,

każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Należy zastanowić się, czy osoba której dane przetwarzane są w podmiocie leczniczym może żądać usunięcia jej danych. Dane medyczne są niezbędne do świadczenia usługi medycznej a zatem brak możliwości przetwarzania tych danych, uniemożliwiłby realizowanie praw do opieki zdrowotnej.

Przechowywanie danych pacjenta zawartych w dokumentacji medycznej stanowi odrębną kategorię prawną w stosunku do przepisów UODO.

Art. 24 i 29 UPrPacjRPP określają obowiązki i terminy przechowywania danych dotyczących pacjenta zawartych w tej dokumentacji. Zgodnie z art. 24 **UPrPacjRPP** w celu realizacji praw pacjenta do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych, podmiot wykonujący działalność leczniczą obowiązany jest do prowadzenia dokumentacji medycznej, (w zakresie wskazanym w art. 25 UPrPacjRPP) którą zgodnie z art. 29 ust. 1 **UPrPacjRPP** zobowiązany jest przechowywać przez okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkiem[9]:

1) dokumentacji medycznej w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym nastąpił zgon;
2) dokumentacji medycznej zawierającej dane niezbędne do monitorowania losów krwi i jej składników, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu;
3) zdjęć rentgenowskich przechowywanych poza dokumentacją medyczną pacjenta, które są przechowywane przez okres 10 lat, licząc od końca roku kalendarzowego, w którym wykonano zdjęcie;
4) skierowań na badania lub zleceń lekarza, które są przechowywane przez okres:

    a) 5 lat, licząc od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza,

    b) 2 lat, licząc od końca roku kalendarzowego, w którym wystawiono skierowanie – w przypadku gdy świadczenie zdrowotne nie zostało udzielone z powodu niezgłoszenia się pacjenta w ustalonym terminie, chyba że pacjent odebrał skierowanie;

5) dokumentacji medycznej dotyczącej dzieci do ukończenia 2. roku życia, która jest przechowywana przez okres 22 lat.

Dopiero po upływie wskazanych powyżej okresów podmiot udzielający świadczeń zdrowotnych niszczy dokumentację medyczną w sposób uniemożliwiający identyfikację pacjenta, którego dotyczyła (art. 29 ust. 2 **UPrPacjRPP).**

[9] https://www.zdrowie.abc.com.pl/artykuly/pacjent-nie-ma-prawa-do-usuniecia-danych-osobowych-ktore-posiada-placowka,15984.html

Uprawnienia pacjenta związane z dokumentacją medyczną określa art. 23 **UPrPacjRPP** według którego pacjent ma prawo do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych, zaś dane zawarte w dokumentacji medycznej podlegają ochronie określonej w tej ustawie oraz w przepisach odrębnych.

Nie obejmuje to zatem prawa pacjenta do żądania usunięcia danych w okresie objętym obowiązkowym przechowywaniem dokumentacji.

W zakresie uprawnień do usunięcia danych osobowych pacjenta zawartych w dokumentacji medycznej **UPrPacjRPP** stanowi lex specialis w stosunku do ustawy o ochronie danych osobowych, odsyłając do tej ostatniej tylko w zakresie odnoszącym się do ochrony tych danych.[10]

Podsumowanie

Prawo do zapomnienia, czyli żądanie usunięcia danych osobowych zawartych w dokumentacji medycznej możliwe jest jedynie w przypadku kiedy okres jej przechowywania upłynie.

4. **Prawo sprzeciwu** – osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych. By skorzystać z tego uprawnienia musi złożyć pisemne umotywowane żądanie zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację. W tej sytuacji administrator jest zobowiązany do zaprzestania przetwarzania, chyba że wykaże istnienie ważnych i prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych nad interesami osoby, której dotyczą. W przypadku danych przetwarzanych w celach marketingowych lub kiedy osoba, której dane dotyczą, chce je przekazać innemu administratorowi, powołanie się na szczególną sytuację nie jest konieczne i w tej sytuacji sprzeciw ma charakter bezwzględny i oznacza, że administrator nie ma prawa podważania sprzeciwu. Osoba, której dane dotyczą nie może skorzystać z prawa sprzeciwu gdy administrator przetwarza dane na podstawie przepisów prawa lub gdy jest to konieczne dla realizacji umowy, której podmiot danych jest stroną. Aktualne przepisy regulujące tę kwestię znajdują się w art. 32 ust. 1 pkt. 7-8 i ust. 2-3[xxii] UODO.
   W sytuacji w której, administrator uzasadni przetwarzanie danych spełnieniem warunków o których mowa w art. 23 ust. 1 pkt 4 i 5 UODO, tj. wtedy, gdy: przetwarzanie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub jest niezbędne do wypełnienia jego prawnie usprawiedliwionych celów, lub osób trzecich, którym dane te przekazuje. Natomiast prawo to nie przysługuje, gdy w sytuacji kiedy podstawą przetwarzania danych jest zgoda, szczególny przepis prawa lub są one przetwarzane w związku z wykonaniem umowy zawartej z administratorem.

[10] Tamże.

W przypadku wniesienia sprzeciwu dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby, w celach objętych sprzeciwem (art. 32 ust. 3 ustawy).[11]

Od 25 maja 2018 r., w zakresie prawa do sprzeciwu odpowiednio stosować będziemy przepisy art. 21[xxiii] RODO.

Zgodnie z art. 21 RODO osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO tj. wtedy gdy: przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem, w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

[11] https://www.gazeta-msp.pl/?id=pokaz_artykul&indeks_artykulu=1084&nr_historyczny=87

5. **Prawa związane z podejmowaniem zautomatyzowanych decyzji** – zgodnie z przepisami o ochronie danych osobowych niedopuszczalne jest rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem zautomatyzowanych operacji na danych osobowych, prowadzonych w systemie informatycznym. Są to przypadki, w których decyzja opiera się wyłącznie na operacjach na danych osobowych, wykonywanych automatycznie przez system informatyczny tj. bez udziału czynnika ludzkiego.[12] Do takiego przetwarzania zalicza się „profilowanie" – które polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa. Niemniej podejmowanie decyzji na podstawie takiego przetwarzania, w tym profilowania, powinno być dozwolone, w przypadku gdy jest to wyraźnie dopuszczone prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, w tym do celów monitorowania i zapobiegania – zgodnie z uregulowaniami, standardami i zaleceniami instytucji Unii lub krajowych podmiotów nadzorujących – oszustwom i uchylaniu się od podatków oraz do zapewniania bezpieczeństwa i niezawodności usług świadczonych przez administratora, lub gdy jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem, lub gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, obejmującym informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji. Takie przetwarzanie nie powinno dotyczyć dzieci.

   W przypadku kiedy jednak podjęto zautomatyzowane decyzje zgodnie z obowiązującymi przepisami prawa, osoba w sprawie której decyzje podjęto ma szczególne prawo pozwalające jej na kontrolowanie omawianego procesu:

   - Prawo do uzyskania informacji o przesłankach podjęcia rozstrzygnięcia,
   - Prawo do żądania ponownego, indywidulanego rozpatrzenia sprawy.

[12] Ochrona danych osobowych medycznych. C.H. Beck, Praca zbiorowa dr inż. K. Wojsyk, dr P. Litwiński, .M. Jagielski, M. Krasińska, P. Kawczyński, 2016 r.

Aktualnie kwestię tę uregulowano w art. 26a[xxiv], art. 32 ust. 1 pkt 5a i pkt 9[xxv] oraz ust 3a[xxvi] UODO a od 25 maja 2018 roku kwestię tę regulować będzie art. 22[xxvii] RODO.

Ważne

UODO wyróżnia pięć typów uprawnień podmiotów danych – prawo do informacji, prawo do poprawienia danych, prawo żądania usunięcia danych, prawo sprzeciwu, oraz prawo związane z podejmowaniem zautomatyzowanych decyzji. Od 25 maja 2018 r. wprowadzone zostaje prawo do przenoszenia danych między administratorami. Jest to powiązane z obowiązkami administratorów, możliwość skorzystania z uprawnienia rodzi po stronie podmiotu zobowiązanego nakaz podjęcia odpowiednich czynności na rzecz uprawnionego.

6. **Prawo do przenoszenia danych** – RODO wprowadza prawo do przenoszenia danych osobowych. Zgodnie z art. 20 RODO – jeżeli przetwarzanie danych: odbywa się na podstawie zgody osoby, której dane dotyczą lub umowy, której stroną jest osoba, której dane dotyczą oraz przetwarzanie odbywa się w sposób zautomatyzowany, osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Wykonując prawo do przenoszenia danych osoba, której dane dotyczą może zażądać od administratora danych by jego dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Z tego prawa można skorzystać jedynie wtedy kiedy dane mają postać elektroniczną i tylko wtedy kiedy administrator przetwarza te dane na podstawie zgody podmiotu danych lub na podstawie zawartej z tym podmiotem umowy.

   Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku dla prawa do usunięcia danych. Prawo do przenoszenia danych nie powinno w szczególności skutkować usunięciem danych osoby, dane dotyczą, a które osoba ta dostarczyła do wykonania umowy, o ile i w takim zakresie, w jakim te dane osobowe są niezbędne do wykonania tej umowy.

   Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Prawa tego – z uwagi na jego charakter – nie powinno się wykonywać w stosunku do administratorów przetwarzających dane osobowe w ramach wykonywania obowiązków publicznych. Dlatego nie powinno ono mieć zastosowania w przypadkach, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

2.2 Obowiązki formalne podmiotów przetwarzających dane medyczne

Podmiot przetwarzający dane osobowe bez względu na przesłanki ich przetwarzania, zobowiązany jest zrealizować wymogi o charakterze formalnym związane z procesem przetwarzania, a wynikające z przepisów prawa.

2.2.1 Wymagania personalne z zakresu ochrony danych osobowych w tym danych medycznych

UODO pozwala administratorom danych działać w jeden z dwóch niżej wymienionych sposobów:

1. Z powołaniem ABI;
2. Bez powołania ABI.

Do zadań Administratora Bezpieczeństwa Informacji należy zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych, nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 1 i 2[xxviii] UODO oraz przestrzegania zasad w niej określonych, zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych, prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów podlegających zgłoszeniu do GIODO.

W przypadku kiedy administrator decyduje się nie powoływać ABI, to za realizację obowiązków z zakresu ochrony danych osobowych odpowiedzialny jest sam administrator danych.

W takiej sytuacji zaleca się aby wyznaczyć przynajmniej osobę lub osoby, które będą zajmować się ochroną danych i będą te zadania miały wpisane w zakres obowiązków służbowych. Należy jednak zaznaczyć, że w przypadku wyznaczenia takich osób pełna odpowiedzialność spoczywa nadal na administratorze danych zgodnie z art. 36b[xxix] UODO.

Wszystkie osoby, które przetwarzają dane osobowe, powinny zostać zidentyfikowane i powinny otrzymać upoważnienia do przetwarzania danych osobowych zgodnie z art. 37[xxx] UODO, jednocześnie powinny zostać zapoznane z przepisami o ochronie danych osobowych. Dobrą praktyką jest aby w celu realizacji wymogów art. 36A ust. 2 pkt 1 lit. c UODO oraz w przyszłości realizacji wymogów art, 39 ust. 1 pkt a i b RODO zapoznanie z przepisami zostało potwierdzone przez pracownika upoważnianego stosownym oświadczeniem a oświadczenie to powinno zostać dołączone do akt osobowych pracownika zgodnie z art. 36a ust. 2 pkt 1 lit. c[xxxi] UODO a od 2018 r zgodnie z art. 39 ust. 1 pkt a i b[xxxii] RODO.

Wszystkie osoby, które zostały upoważnione i dopuszczone do przetwarzania danych osobowych, powinny zostać zobowiązane do zachowania danych oraz sposobu ich zabezpieczenia w tajemnicy jednocześnie zapewniając spisanie potwierdzenia takiego zobowiązania oraz dołączenia go do akt pracowniczych , zgodnie z art. 39 ust. 2[xxxiii] UODO.

Od 25 maja 2018 r. zgodnie z RODO Administrator Bezpieczeństwa Informacji zostanie zastąpiony inspektorem ochrony danych osobowych (IOD).

Podobnie jak w ramach obowiązującej nadal UODO powołanie IOD nie jest obligatoryjne. W RODO przewidziano trzy przypadki, kiedy Administrator danych lub podmiot przetwarzający dane osobowe powinny wyznaczyć IOD.

Zgodnie z art. 37 RODO Administrator i podmiot przetwarzający wyznaczają IOD, zawsze gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO tj. danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

RODO w art. 37 ust. 5 - IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO tj. zadań Inspektora ochrony danych.

Zgodnie z art. 37 ust 6 RODO IOD może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

W dniu 5 kwietnia 2017 r. Grupa Robocza art. 29 przyjęła zmienione Wytyczne dotyczące inspektorów ochrony danych.

Grupa Robocza art. 29 wskazuje w wytycznych, iż w świetle RODO IOD ma kluczowe znaczenie w procesie administrowania danymi w związku z czym w rozporządzeniu określono warunki jego powołania, status i opis zadań. Grupa Robocza art. 29 postawiła sobie za cel wytycznych, wyjaśnienie stosownych zapisów RODO celem ułatwienia administratorom i podmiotom przetwarzającym dostosowania się do przepisów prawa, jak również ułatwienia inspektorom ochrony danych wykonywania ich zadań. Grupa Robocza art. 29 zawarła w wytycznych również zalecane dobre praktyki, oparte na doświadczeniu niektórych państw członkowskich. Grupa Robocza art. 29 zadeklarowała, iż będzie na bieżąco monitorować implementację wytycznych i w razie zaistnienia potrzeby wzbogacać je o dalsze informacje.

RODO nie przedstawia definicji pojęcia „organu lub podmiotu publicznego”. Grupa Robocza art. 29 w wytycznych dotyczących inspektorów danych osobowych z dnia 5 kwietnia 2017 r. wskazała, że takie pojęcie powinno zostać określone na poziomie przepisów krajowych. Do organów lub podmiotów

publicznych najczęściej zalicza się organy władzy krajowej, organy regionalne i lokalne, ale również – na mocy właściwego prawa krajowego - szereg innych podmiotów prawa publicznego. We wszystkich tych przypadkach powołanie IOD będzie obowiązkowe.

Zadanie może być realizowane w interesie publicznym lub może być sprawowana władza publiczna nie tylko przez organy lub podmioty publiczne, ale również przez inne osoby fizyczne i prawne podlegające prawu publicznemu lub prywatnemu, w sektorach takich jak np. transport publiczny, dostarczanie wody i energii, infrastruktura drogowa, radiofonia i telewizja, budynki użyteczności publicznej albo organy powołane dla zawodów regulowanych.

W tych przypadkach sytuacja osób, których dane dotyczą może być bardzo podobna do sytuacji przetwarzania ich danych przez organy lub podmioty publiczne. W szczególności dane mogą być przetwarzane w podobnych celach, a możliwość wpływu osób, których dane dotyczą, na charakter tego przetwarzania może być ograniczona bądź wyłączona, co może wymagać dodatkowej ochrony, jaką daje powołanie IOD.

Choć w powyższych przypadkach obowiązek powołania IOD nie wynika z RODO, to Grupa Robocza Art. 29 zaleca w ramach dobrych praktyk powoływanie IOD przez prywatne jednostki realizujące zadania w interesie publicznym lub sprawujące władzę publiczną. Działalność IOD powinna obejmować również wszelkie operacje przetwarzania prowadzone przez jednostkę, w tym te niezwiązane z zadaniami realizowanymi w interesie publicznym.

Artykuł 37 ust. 1 pkt. b i c RODO zawiera zwrot „główna działalność administratora lub podmiotu przetwarzającego”. Zgodnie z motywem 97 RODO przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności. Tak więc „główną działalnością” będzie działalność kluczowa z punktu widzenia osiągnięcia celów administratora albo podmiotu przetwarzającego dane.

„Głównej działalności” nie należy interpretować w sposób wyłączający działalność w zakresie przetwarzania danych nierozerwalnie związaną z działalnością główną. Dla przykładu działalnością główną szpitali będzie zapewnianie opieki medycznej. Natomiast prowadzenie efektywnej opieki medycznej nie byłoby możliwe bez przetwarzania danych medycznych jak np. historii choroby pacjenta. W związku z tym działalność polegająca na przetwarzaniu historii choroby pacjenta również powinna zostać zaklasyfikowana jako działalność główna. Oznacza to, że szpitale będą miały obowiązek powołania IOD.

Jednocześnie Grupa Robocza Art. 29 jest świadoma, że wszystkie podmioty, spółki i inne organizacje prowadzą określone działania, np. prowadząc listę płac albo korzystając z obsługi IT. Są to niezbędne działania umożliwiające prowadzenie działalności głównej, jednak z racji na ich charakter uznane są za poboczne.

Artykuł 37 ust. 1 pkt. b i c RODO uzależnia obowiązek powołania IOD od przetwarzania danych osobowych na „dużą skalę”. I choć RODO nie definiuje tego pojęcia, to pewne wskazówki znajdują się w motywie 91.

Nie jest możliwe wskazanie konkretnej wartości, czy to rozmiaru zbioru danych, czy liczby osób, których dane dotyczą, która determinowałaby „dużą skalę”. Nie wyklucza to sytuacji, w której wraz z rozwojem

praktyki ukształtują się standardy, które umożliwiałyby kwantytatywne określenie „dużej skali" w odniesieniu do określonych rodzajów przetwarzania. Grupa Robocza Art. 29 zamierza wspierać ten proces poprzez rozpowszechnianie przykładów odpowiednich progów dla wyznaczenia IOD.

W każdym razie, Grupa Robocza art. 29 zaleca uwzględnianie następujących czynników przy określaniu, czy przetwarzanie następuje na „dużą skalę": Liczba osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa; zakres przetwarzanych danych osobowych; okres, przez jaki dane są przetwarzane; zakres geograficzny przetwarzania danych osobowych;

Do przykładów „przetwarzania na dużą skalę" zaliczyć można: przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności; przetwarzanie danych osób korzystających ze środków komunikacji miejskiej (np. śledzenie za pośrednictwem kart miejskich; przetwarzanie danych geolokalizacyjnych w czasie rzeczywistym przez wyspecjalizowany podmiot do celów statystycznych; przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności; przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki; przetwarzanie danych (dotyczących treści, ruchu, lokalizacji) przez dostawców usług telefonicznych lub internetowych.

Przykłady przetwarzania niemieszczącego się w definicji „dużej skali":

- przetwarzanie danych pacjentów – klientów, dokonywane przez pojedynczego lekarza prowadzącego indywidulaną praktykę lekarską;

- przetwarzanie danych dotyczących wyroków skazujących lub naruszeń prawa przez adwokata lub radcę prawnego.

Ważne

Administrator danych osobowych kierując się wskazówkami Grupy Roboczej Art. 29 powinien przeanalizować przesłanki obligatoryjnego powołania IOD i na tej podstawie podjąć stosowną decyzję.

2.2.2. Obowiązki rejestracyjne

Zgodnie z art. 40[xxxiv] UODO administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Zgodnie z art. 43[xxxv] UODO ustawodawca przewidział przypadki zbiorów, w których administratorzy zwolnieni są z obowiązku ich rejestracji.

Ważne

Od 25 maja 2018 r. całkowicie znika obowiązek rejestracji zbiorów w tym zbiorów danych wrażliwych. Zastępuje go rejestr czynności przetwarzania prowadzony przez Administratora danych osobowych.

Należy szczególnie zwrócić uwagę na fakt, że zwolnienie z prowadzenia rejestru przetwarzania nie dotyczy sytuacji w której w podmiocie przetwarzane są dane wrażliwe np. dane o stanie zdrowia.

RODO nie przewiduje obowiązku zgłaszania zbiorów danych osobowych do GIODO. Wprowadza jednak obowiązek prowadzenia wewnętrznego rejestru przetwarzania. Zawartość rejestru określona jest w art. 30 ust. 1 RODO.

W rejestrze zamieszcza się następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO tj. pseudonimizacja i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Rejestr zobowiązani są prowadzić nie tylko administratorzy, ale także każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego zdefiniowany w art. 4 RODO (np. firmy utrzymujące systemy informatyczne, usługodawcy usług chmury obliczeniowej, dostawcy usług hostingu).

Zgodnie z art. 30 ust. 2 RODO, każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO tj. pseudonimizacja i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Ważne

Podmioty medyczne przetwarzają dane wrażliwe i przetwarzanie ich stwarza ryzyko naruszenia praw i wolności osób, których dane dotyczą a więc są zobowiązane do prowadzenia rejestru.

Rejestr można prowadzić opierając się na dotychczasowej dokumentacji procesu przetwarzania danych osobowych prowadzonej na podstawie UODO oraz DokPrzetwR.

Dokumentacja ta wymagała będzie aktualizacji i dostosowania do wymagań RODO, ale stanowi źródło informacji, które ułatwią sprawne kompletowanie dokumentów pozwalających na właściwe rozliczenie się administratora i procesora z wykonywanych czynności w ramach realizowanej umowy powierzenia.

Formalnie, zgodnie z art. 30 ust. 5 RODO, z obowiązku prowadzenia rejestru przetwarzania zwolnieni będą przedsiębiorcy i podmioty zatrudniające mniej niż 250 osób. Wyłączenie to nie ma jednak zastosowania, gdy przetwarzanie, którego dokonują:

a) „może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą” (np. ryzyko ujawnienia danych osobom niepowołanym);
b) „nie ma charakteru sporadycznego” (a więc następuje regularnie, choćby w niewielkiej skali) lub
c) obejmuje szczególne kategorie danych osobowych, o których mowa w art. 10.

Zwolnienie jest więc sformułowane na tyle wąsko, że obowiązek prowadzenia rejestru będzie prawdopodobnie dotyczył znakomitej większości przedsiębiorców przetwarzających dane osobowe (klientów, pracowników, etc.).

2.2.3. Sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

W obecnym stanie prawnym tj. do dnia 24 maja 2018 r. każdy podmiot przetwarzający dane osobowe jest zobowiązany przygotować plan sprawdzeń obejmujący minimalnie kwartał, a maksymalnie rok. Plan sprawdzeń musi określać przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania. Plan musi przewidywać przynajmniej jedno sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Plan sprawdzeń musi obejmować w szczególności zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz weryfikację zgodności przetwarzania danych osobowych z zasadami i obowiązkiem wynikającym z § 3 ust. 4 rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 r. poz. 745). Każdy zbiór danych osobowych oraz każdy system informatyczny służący do przetwarzania danych osobowych musi być objęty sprawdzeniem co najmniej raz na pięć lat. Należy pamiętać, że oprócz planowych sprawdzeń ABI dokonuje sprawdzeń doraźnych w przypadku podejrzenia niezgodności w zakresie przetwarzania danych osobowych. Jeśli administrator powołał ABI, to realizacja sprawdzeń jest obowiązkiem ABI. Jeśli administrator nie powołał ABI, to sprawdzeń dokonuje administrator danych. Zagadnienia dotyczące sprawdzeń szczegółowo reguluje wyżej powołane rozporządzenie.

Wskazać także należy, że zgodnie z art. 19b ust. 1 UODO, organ nadzorczy może zwrócić się do administratora bezpieczeństwa informacji, o dokonanie sprawdzenia, u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia.

Sprawdzenia obejmują cztery elementy:

1. Inwentaryzację zbiorów,
2. Sprawdzenie, czy są realizowane obowiązki z ustawy o ochronie danych osobowych UODO,
3. Sprawdzenie, czy zbiory i systemy przetwarzające dane osobowe są odpowiednio zabezpieczone,
4. Weryfikację i aktualizację dokumentacji z zakresu ochrony danych osobowych oraz weryfikację przestrzegania zasad i procedur w niej zawartych.

Inwentaryzacja zbiorów polega na ustaleniu stanu rzeczywistego tj. identyfikacji jakie dane są w posiadaniu administratora, w jakich zbiorach są przetwarzane, jakie systemy informatyczne wykorzystywane są do przetwarzania danych.

Obowiązek przeprowadzenia inwentaryzacji wynika pośrednio z § 3 ust. 4[xxxvi] Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r (Dz. U. z 2015, poz. 745).

Analiza realizacji obowiązków wynikających z UODO to kolejny element, który powinien podlegać sprawdzeniu. W ramach tej czynności weryfikacji podlega:

1. legalność przetwarzania danych osobowych zgodnie z zasadami określonymi w art. 23[xxxvii] UODO;
2. legalność przetwarzania danych osobowych wrażliwych zgodnie z zasadami określonymi w art. 27[xxxviii] UODO;
3. spełnienie wymogów celowości przetwarzania danych osobowych zgodnie z art. 26[xxxix] UODO;
4. merytoryczna poprawność i adekwatność celów w jakich są przetwarzane dane osobowe;
5. przestrzeganie zakazu podejmowania zautomatyzowanych decyzji, o którym mowa w art. 26a[xl] UODO;
6. obowiązki informacyjne związane ze zbieraniem danych osobowych zgodnie z art. 24[xli] i art. 25[xlii] UODO;
7. przestrzeganie praw osób, których dane dotyczą zgodnie z art. 7 pkt 5[xliii], art. 32 ust. 1 pkt 1-5a[xliv] oraz art. 33[xlv]-34[xlvi], art. 32 ust. 1 pkt 6 [xlvii]oraz art. 35[xlviii], art. 32 ust. 1 pkt 7 art. 32 ust. 1 pkt 8 oraz pkt 9[xlix] UODO;
8. realizacja obowiązku zgłoszenia zbioru lub ABI do GIODO zgodnie z art. 40[l] i 43[li]UODO;
9. realizacja obowiązku prowadzenia rejestru zbiorów zgodnie z art. 36a ust. 2 pkt 2 UODO;
10. realizacja obowiązku sprawowania kontroli nad upoważnieniami i przekazaniem danych zgodnie z art. 39 ust. 1 UODO;
11. realizacja obowiązku prowadzenia ewidencji osób upoważnionych zgodnie z art. 39 ust. 1 UODO;
12. moment, w którym rozpoczęto przetwarzanie danych w zbiorach podlegających rejestracji zgodnie z art. 46[lii] UODO;
13. realizacja obowiązków w zakresie przekazywania danych za granicę zgodnie z art. 47[liii] i art. 48[liv] UODO;
14. realizacja obowiązków w zakresie powierzenia przetwarzania danych innemu podmiotowi zgodnie z art. 31[lv] UODO.

W trakcie sprawdzeń należy dokonać weryfikacji zabezpieczenia zbiorów danych osobowych i systemów informatycznych przetwarzających dane osobowe.

Kontrola zabezpieczeń w zakresie bezpieczeństwa fizycznego powinna obejmować sprawdzenie następujących elementów: zabezpieczenie obiektów, pomieszczeń i dokumentacji, w których znajdują się dane osobowe, zbiorów danych osobowych, systemów informatycznych, nośników, na których przechowywane są kopie bezpieczeństwa oraz pomieszczeń, w których zlokalizowane są urządzenia sieciowe, serwery i stacje robocze. Oznacza to konieczność sprawdzenia nie tylko przestrzegania zasad ochrony fizycznej ale także sprawdzenia działania systemów antywłamaniowych i przeciwpożarowych, zabezpieczenia okien i drzwi oraz sposobu zabezpieczenia szaf.

Kontrola zabezpieczeń w zakresie bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym powinna obejmować weryfikację spełnienia wymagań określonych w § 6[lvi] DokPrzetwR.

Sprawdzenie musi obejmować także weryfikację realizacji procedur szczególnych określonych w § 5[lvii] i § 7[lviii] DokPrzetwR tj.:

1. nadawanie uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2. stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3. procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5. sposób, miejsce i okres przechowywania:
   a) elektronicznych nośników informacji zawierających dane osobowe,

   b) kopii zapasowych, o których mowa w pkt 4.

6. sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia DokPrzetwR;
7. sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4[lix] DokPrzetwR ;
8. procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Weryfikacja i aktualizacja dokumentacji z zakresu ochrony danych osobowych oraz weryfikacja przestrzegania zasad i procedur w niej zawartych polega na sprawdzeniu, zgodnie z § 7 ust. 1[lx] DokPrzetwR, czy opracowano oraz czy jest kompletna dokumentacja przetwarzania danych, w tym:

1. czy dokumentacja zgodna jest z obowiązującymi przepisami prawa;
2. czy przewidziane w dokumentacji środki ochrony technicznej i organizacyjnej służące przeciwdziałaniu zagrożeniom są zgodne ze stanem rzeczywistym;
3. czy przestrzegane są zasady, procedury i obowiązki wynikające z tej dokumentacji.

Zakres dokumentacji, jaka powinna być prowadzona zgodnie z przepisami o ochronie danych osobowych wskazany został w § 3 ust. 1DokPrzetwR[lxi]. Na dokumentację, o której mowa w zdaniu poprzednim składa się Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

1. Polityka bezpieczeństwa zawiera w szczególności:
   - 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 struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
   - sposób przepływu danych pomiędzy poszczególnymi systemami;
   - określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

2. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zawiera w szczególności:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
- sposób, miejsce i okres przechowywania:
  - elektronicznych nośników informacji zawierających dane osobowe,
  - kopii zapasowych, o których mowa w pkt 4,
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- sposób realizacji wymogów w zakresie odnotowywania przez system informacji o odbiorcach, w rozumieniu art. 7 pkt 6lxii UODO, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Do pozostałych dokumentów jakie powinny być opracowywane w związku z przetwarzaniem danych osobowych należy zaliczyć:

3. Indywidulane upoważnienia do przetwarzania danych osobowych zgodnie z art. 37[lxiii] UODO.
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych zgodnie z art. 39[lxiv] UODO.
5. Plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych zgodnie z § 3 ust. 3[lxv] Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015, poz. 745).
6. Program poszczególnych sprawdzeń zaplanowanych zgodnie z planem sprawdzeń.
7. Sprawozdania z poszczególnych sprawdzeń lub dokumentacja poszczególnych sprawdzeń w zależności od tego czy powołano czy nie ABI.

Zgodnie z art. 39 ust. 1 pkt b RODO IOD odpowiedzialny będzie za monitorowanie przestrzegania przepisów RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty. Jak z powyższego wynika nie ogranicza się on wyłącznie do monitorowania zgodności przetwarzania danych z przepisami RODO ale monitorowanie to musi uwzględniać inne przepisy w tym przepisy krajowe, wewnętrzne dokumenty organizacji.

Ważne

Ryzyko należy analizować znacznie szerzej w odniesieniu do wszystkich praw i wolności osób fizycznych, a nie jedynie jako prawa związanego z tym, że dane osobowe będą przetwarzane przez administratora w sposób bezpieczny.

Monitorowanie przestrzegania zgodności przetwarzania danych z przepisami o ochronie danych osobowych wiąże się z przeprowadzaniem przez IOD audytów ochrony danych osobowych. Przepisy RODO jedynie nakreślają ogólny zakres działań, które IOD musi podjąć, aby zapewnić bezpieczeństwo przetwarzania danych. Na chwilę obecną brak jest wytycznych opisujących sposób lub tryb wykonywania tych zadań. Jednak zgodnie z ogólną zasadą podejścia opartego na ryzyku, podmiot przetwarzający dane osobowe będzie musiał wdrożyć odpowiednie zabezpieczenia zarówno w warstwie systemowej, organizacyjnej i technicznej, które zapewnią należytą ochronę danych osobowych.

2.2.4. Ocena skutków ochrony danych osobowych – analiza oparta na ryzyku

RODO wprowadza nowy obowiązek dla administratora danych polegający na dokonywaniu oceny skutków dla ochrony danych (ang. Data Protection Impact Assessment „DPIA"). Oceny skutków dokonujemy w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

Ważne

Weryfikacja i aktualizacja dokumentacji z zakresu ochrony danych osobowych oraz weryfikacja przestrzegania zasad i procedur w niej zawartych polega na sprawdzeniu, czy dokumentacja przetwarzania danych jest opracowana i kompletna, oraz czy:

1. **Dokumentacja zgodna jest z obowiązującymi przepisami prawa?**
2. **Przewidziane w dokumentacji środki ochrony technicznej i organizacyjnej służące przeciwdziałaniu zagrożeniom są zgodne ze stanem rzeczywistym?**
3. **Przestrzegane są zasady, procedury i obowiązki wynikające z tej dokumentacji?**

W myśl art. 35 ust. 1 RODO jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Zgodnie z przepisami RODO obowiązkiem podmiotu przetwarzającego dane osobowe jest ustalenie, czy dany rodzaj przetwarzania powodować może wysokie ryzyko naruszenia ochrony danych osobowych.

Zgodnie z art. 35 ust. 3 ocena skutków dla ochrony danych, jest wymagana w szczególności w przypadku:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych wrażliwych (pochodzenie rasowe, etniczne, poglądy, wyznanie, dane dotyczące zdrowia itp.) lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa;
c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Z treści RODO wynika, że nie w każdym przypadku dokonanie oceny będzie konieczne. Kryterium stanowić będzie duże prawdopodobieństwo spowodowania ryzyka naruszenia praw lub wolności osób fizycznych. Każdy administrator przed planowanym przetwarzaniem danych będzie musiał sam ocenić czy ono występuje.

Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Poniżej wskazano przykłady operacji przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Należy jednak pamiętać, że są to przykłady i nie stanowią zamkniętego katalogu operacji przetwarzania związanych z wysokim ryzykiem naruszenia praw i wolności osób fizycznych.

Profilowanie, przewidywanie czy wnioskowanie

Profilowanie, przewidywanie czy wnioskowanie, w szczególności w zakresie danych osób fizycznych, które pozwalają oceniać lub prognozować w zakresie sytuacji ekonomicznej, osobistych preferencji w tym preferencji seksualnych, obecnego i przyszłego stanu zdrowia, zainteresowań, wyznania lub zainteresowań, przemieszczania się osoby [motyw 71 i 91 preambuły RODO]. Jest to przetwarzanie mające na celu podejmowanie decyzji, które mogą prowadzić do dyskryminacji i wykluczenia osób. Przykładem może być wyższa cena biletów z powodu wyznania czy nadwagi, wyższe ceny ubezpieczenia czy odrzucenie elektronicznie złożonego wniosku o kredyt.

Jak wskazano w publikacji „Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji" Jędrzeja Niklasa profilowanie może prowadzić do naruszenia prywatności nie tylko gdy tworzy się indywidualny profil, ale również kwalifikuje osobę do określonej grupy. Z perspektywy autonomii informacyjnej istotne jest to, że profilujący wie, że osoba należy do określonej kategorii (np. osób homoseksualnych, osób z nadwagą) i jest w stanie tę wiedzę wykorzystać na swoją korzyść. Obecnie istnieją ku temu możliwości techniczne. Niedawne badania przeprowadzone na Uniwersytecie w Cambridge, wykazały, że analiza danych umieszczanych na Facebooku pozwala wykazać, w znaczącej większości przypadków, orientację seksualną danej osoby, pomimo, że ona tej informacji nie ujawnia[13].

Systematyczne monitorowanie

Przetwarzanie danych wykorzystywane do obserwowania, monitorowania lub kontrolowania określonych osób fizycznych, w tym danych gromadzonych za pomocą monitoringu wizyjnego miejsc publicznych (np. parkingu przed szpitalem) [art. 35 ust. 3 lit. c, RODO]. Dane osobowe nie mogą być zbierane w okolicznościach, w których osoby fizyczne, których dane dotyczą, nie wiedzą o tym, nie wiedzą kto gromadzi dane i jak będą one wykorzystywane. Jest to także sytuacja, w której nie można uniknąć tych miejsc publicznych, a zatem nie można uniknąć przetwarzania danych.

Przetwarzanie danych wrażliwych w tym danych o stanie zdrowia

Szczególna kategoria danych osobowych, o których mowa w art. 9 RODO. Należą do nich m.in. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Przetwarzanie danych na dużą skalę

[13]http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekscie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf

RODO nie określa, co stanowi dużą skalę, chociaż w motywie 91 preambuły RODO przedstawiono wytyczne w tym zakresie. Zaleca się, aby przy określaniu, czy przetwarzanie jest przeprowadzane na dużą skalę, w szczególności rozważać następujące czynniki:

a) liczbę osób fizycznych, których dane osobowe są przetwarzane;
b) ilość danych osobowych i/lub zakres przetwarzania danych;
c) czas trwania lub trwałość przetwarzania danych osobowych;
d) geograficzny zakres działalności związanej z przetwarzaniem.

Do przykładów „przetwarzania na dużą skalę" zaliczyć można przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności, przetwarzanie danych dotyczących podróży osób korzystających ze środków komunikacji miejskiej (np. śledzenie za pośrednictwem „kart miejskich", przetwarzanie danych geolokalizacyjnych klientów w czasie rzeczywistym przez wyspecjalizowany podmiot na rzecz międzynarodowej sieci fast food do celów statystycznych, przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności, przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki, przetwarzanie danych (dotyczących treści, ruchu, lokalizacji) przez dostawców usług telefonicznych lub internetowych.

Przetwarzanie danych dzieci, osób starszych, pacjentów, osób chorych psychicznie.

Przetwarzanie tego rodzaju danych osobowych może wymagać oceny skutków dla ochrony danych osobowych z powodu nierównowagi między osobą fizyczną, której dane osobowe dotyczą a administratorem danych. Dzieci mogą być uważane za nieumiejętne w sprzeciwianiu się lub nie wyrażeniu zgody na przetwarzanie ich danych.

Ważne

RODO nie wskazuje jak dokładnie ma przebiegać ocena. W treści motywu 84 preambuły RODO stwierdzono, iż ocena skutków przetwarzania danych osobowych ma na celu oszacowanie w szczególności źródła, charakteru, specyfiki i powagi ryzyka naruszenia praw lub wolności osób fizycznych związanego z przetwarzaniem danych osobowych. Natomiast w myśl motywu 90 preambuły RODO, ocena skutków powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające minimalizować to ryzyko, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie RODO.

Przetwarzanie z wykorzystaniem nowych technologii

Wykorzystanie nowych technologii lub rozwiązań może wiązać się z nowatorskimi formami gromadzenia i wykorzystania danych, co może powodować duże zagrożenie dla praw i wolności jednostek. Na przykład połączenie użycia skanowania siatkówki oka i rozpoznawania twarzy w celu poprawy fizycznej kontroli dostępu.

Przetwarzanie danych polegające na przekazywaniu danych poza obszar Unii Europejskiej

Należy pamiętać, że im bardziej spełniane są powyższe kryteria, tym bardziej prawdopodobne jest, że stwarzają one ryzyko naruszenia praw i wolności osób fizycznych, których dane osobowe dotyczą, a

Ważne

W trakcie przetwarzania danych może zajść konieczność aktualizacji oceny ryzyka. W dynamicznych lub często zmieniających się operacjach przetwarzania danych aktualizacja oceny skutków przetwarzania może okazać się konieczna dla rzeczywistego zapewnienia należytej ochrony przetwarzania danych.

zatem wymagają przeprowadzenia oceny skutków dla ochrony danych osobowych.

W przypadku danych medycznych spełnione zostaje kryterium wysokiego ryzyka naruszenia praw i wolności, a to wymaga przeprowadzenia oceny skutków dla ochrony danych osobowych.

Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.

Jeżeli zaś chodzi o treść oceny to jej niezbędne elementy określa przepis art. 35 ust. 7 RODO . Ocena skutków przetwarzania obligatoryjnie zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Zgodnie z treścią art. 36 ust. 1 RODO jeżeli ocena skutków przetwarzania dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym. Zatem jeżeli okaże się, że brak jest środków pozwalających na zminimalizowanie zidentyfikowanego ryzyka to przed przystąpieniem do przetwarzania danych konieczna będzie konsultacja z organem nadzorczym.

W dniu 4 kwietnia 2017 r. Grupa Robocza Art. 29 wydała wytyczne związane ze stosowaniem art. 35 GDPR oraz wymogi wynikające z tego artykułu (w szczególności obejmujące rozumienie pojęcia „wysokiego ryzyka naruszenia praw lub wolności osób fizycznych").

Wytyczne zaproponowane przez Grupę Roboczą określają kryteria, z którymi będzie wiązała się konieczność stosowania regulacji z art. 35 RODO.

Jeżeli operacje na danych będą się wiązały z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych oraz jeżeli zostaną spełnione inne kryteria, dla ochrony danych osobowych obowiązkowe będzie przeprowadzenie oceny skutków przetwarzania. Należy zaznaczyć, iż pojęcie „praw i wolności osób fizycznych" odnosi się w szczególności do prawa do prywatności, ale także do prawa do wolności wypowiedzi, swobody poruszania się, zakazu dyskryminacji, swobody myśli, prawa do wolności i swobody przekonań oraz poglądów religijnych.

Wśród kryteriów zastosowania oceny skutków dla ochrony danych znajdują się m.in. następujące przesłanki:

a) czy przetwarzane dane podlegają profilowaniu (m.in. czy dokonywana jest ocena lub przyznawana jest punktacja na podstawie przewidywań administratora w związku z profilowaniem danych, szczególnie jeżeli prognozowanie dotyczy efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – motywy 71 i 91 preambuły RODO;
b) czy przetwarzanie danych obejmuje automatyczne podejmowanie decyzji, które wywierają znaczący wpływ na prawa osoby, której dane dotyczą;
c) czy wykonywany jest systematyczny monitoring na dużą skalę miejsc dostępnych publicznie;
d) czy przetwarzane są dane szczególnych kategorii, o których mowa w art. 9 i 10 RODO tj. dane wrażliwe lub dane dotyczące wyroków skazujących, naruszeń prawa lub związanych z tym środków bezpieczeństwa;
e) czy zbiory danych podlegają łączeniu;
f) czy dane osobowe są przetwarzane z wykorzystaniem innowacyjnych technologii lub z wykorzystaniem innowacyjnych środków organizacyjnych, w szczególności dotyczących identyfikacji osób fizycznych z zastosowaniem linii papilarnych lub z wykorzystaniem biometrii;
g) czy dane są przekazywane poza UE;
h) czy dane są przetwarzane na wielką skalę;
i) czy operacje przetwarzania utrudniają osobom, których dane dotyczą, wykonywanie przysługującym ich praw.

Wytyczne wskazują również, że w celu zastosowania mechanizmów wynikających z art. 35 RODO należy spełnić przynajmniej dwie z powyższych przesłanek. Czasami jednak w przypadku spełnienia tylko jednej przesłanki możliwe będzie zastosowanie DPIA pod warunkiem, że będzie to uzasadnione okolicznościami danego przypadku.

2.3. Formalnoprawne uwarunkowania w zakresie outsourcingu

Przepisy krajowe i unijne dopuszczają zlecanie przetwarzania danych osobowych podmiotowi zewnętrznemu zajmującemu się profesjonalnym przetwarzaniem danych:

a) Zgodnie z art. 17 ust. 3[lxvi] Dyrektywy 95/46/WE, przetwarzanie danych musi być uregulowane w formie umowy lub aktu prawnego, na mocy którego przetwarzający dane podlega administratorowi danych. Z dokumentu tego musi wynikać, że przetwarzający działa wyłącznie na polecenie administratora danych oraz że ma obowiązek wprowadzić środki techniczne i organizacyjne wymagane do zapewnienia ochrony danych,

b) Zgodnie z art. 31 ust. 1[lxvii] UODO administrator danych może powierzyć przetwarzanie danych innemu podmiotowi w drodze umowy zawartej na piśmie. Zgodnie z art. 31 ust. 2 UODO podmiot, któremu powierzono przetwarzanie danych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Oznacza to że umowa powinna określać cel oraz czynności związane z przetwarzaniem danych, które są powierzane,

c) Zgodnie z art. 28[lxviii]RODO, jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora,

d) UODO w art. 27 ust. 2 pkt 7[lxix] określa, kiedy możliwe jest przetwarzanie danych o stanie zdrowia. Przepis ten wskazuje, że przetwarzanie danych o stanie zdrowia jest dopuszczalne w celu jego ochrony, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych, gdy są stworzone pełne gwarancje ochrony danych osobowych,

e) Zgodnie z art. 24 UPrPacjRPP ustawodawca dopuszcza możliwość przetwarzania danych osobowych przez podmiot udzielający świadczeń zdrowotnych. W myśl art. 24 ust. 4[lxx] UPrPacjRPP podmiot udzielający świadczeń zdrowotnych może zawrzeć umowę, o której mowa w art. 31 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), pod warunkiem zapewnienia ochrony danych osobowych oraz prawa do kontroli przez podmiot udzielający świadczeń zdrowotnych zgodności przetwarzania danych osobowych z tą umową przez podmiot przyjmujący te dane. Zgodnie z art. 24 ust 2[lxxi] UPrPacjRPP osoby wykonujące zawód medyczny oraz inne osoby, wykonujące 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, są uprawnione do przetwarzania danych zawartych w dokumentacji medycznej, o której mowa w art. 25 powołanej ustawy, w celu ochrony zdrowia, udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, utrzymania systemu

teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna i zapewnieniem bezpieczeństwa tego systemu.

Uprawnienie do przetwarzania danych medycznych nie oznacza zwolnienia osób wykonujących zawód medyczny, w tym udzielających świadczeń zdrowotnych, z obowiązku zachowania tajemnicy, o której mowa w art. 13 UPrPacjRPP. Zgodnie z art. 24 ust. 6 UPrPacjRPP, podmiot któremu powierzono przetwarzanie danych o stanie zdrowia, jest zobowiązany do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w wyniku wykonywania umowy powierzenia, również po śmierci pacjenta.

Konstrukcja przepisów art. 24 ust. 6 UPrPacjRPP oznacza, że podmiot przetwarzający na zlecenie ADO, dane osobowe objęte tajemnicą na zasadach art. 13 UPrPacjRPP ma prawny obowiązek zachowania tych danych w tajemnicy, tak jak ADO.

Art. 24 ust. 5 UPrPacjRPP wprowadza zasadę, zgodnie z którą realizacja umowy powierzenia nie może powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej.

Warunkiem, od którego powołana wyżej ustawa uzależnia możliwość zawarcia umowy powierzenia przetwarzania danych medycznych, jest:

a) zapewnienie ochrony danych osobowych. Wymóg taki zawarty jest również w art. 31 ust. 3 UODO, który wskazuje, że podmiot przetwarzający dane osobowe na podstawie umowy powierzenia jest obowiązany, przed rozpoczęciem przetwarzania danych, podjąć środki zabezpieczające dane oraz spełnić wymagania określone w przepisach wykonawczych do UODO.
b) podmiot udzielający świadczeń zdrowotnych, zgodnie z art. 24 UPrPacjRPP, ma obowiązek zapewnienia sobie w umowie powierzenia prawa do kontroli zgodności przetwarzania danych osobowych z tą umową przez podmiot przyjmujący dane.
c) zgodnie z art. 24 ust. 5 UPrPacjRPP realizacja umowy powierzenia, nie może powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej.
d) zgodnie z art. 24 ust. 7 UPrPacjRPP w przypadku zaprzestania przetwarzania danych osobowych zawartych w dokumentacji medycznej przez podmiot, któremu powierzono takie przetwarzanie, w szczególności w związku z jego likwidacją, jest on zobowiązany do przekazania danych osobowych zawartych w dokumentacji medycznej podmiotowi, który powierzył przetwarzanie danych osobowych.

Na gruncie UODO kwestia umowy powierzenia uregulowana jest w art. 31 UODO.

Artykuł 31 UODO wskazuje, że administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie powierzenia i jest zobowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające, o których mowa w art. 36-39 UODO, oraz spełnić

wymagania określone w przepisach wydanych na podstawie delegacji ustawowej zawartej w art. 39a UODO. W zakresie przestrzegania ww. przepisów podmiot przetwarzający dane osobowe na podstawie umowy powierzenia ponosi odpowiedzialność jak administrator danych.

Należy mieć na uwadze, że odpowiedzialność za przestrzeganie przepisów UODO spoczywa na administratorze danych, co nie wyłącza odpowiedzialności procesora za przetwarzanie danych niezgodnie z umową powierzenia. Sposób realizacji kontroli, uprawnienia kontrolne, środki stosowane po kontroli, zostały uregulowane w art. 14 - 19 UODO.

Na podmiocie przetwarzającym dane ciążą dwa rodzaje odpowiedzialności:

a) Odpowiedzialność wynikająca z umowy powierzenia zawartej z administratorem danych. Najważniejszym obowiązkiem procesora, jest stosowanie się do wytycznych i wymagań administratora wynikających z umowy powierzenia, a w szczególności dotyczących zakresu i celu przetwarzania danych. UODO stanowi, że procesor odpowiada przed administratorem danych za przetwarzanie danych osobowych niezgodnie z umową;
b) Odpowiedzialność ustawowa – na procesorze ciąży obowiązek zabezpieczenia danych jeszcze przed rozpoczęciem przetwarzania w myśl art. 31 ust. 3 UODO.

Zgodnie z art. 28 RODO jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. Za wystarczającą gwarancję, podmiot przetwarzający może wykazać między innymi stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40[lxxii] RODO lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42[lxxiii] tego rozporządzenia.

Wynika z tego, że RODO nakazuje administratorowi danych dołożyć szczególnej staranności przy wyborze procesora.

Powierzenie danych osobowych następuje w trybie art. 28 ust. 3 RODO, który stanowi, że przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 RODO;
e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;
f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;
g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

W związku z obowiązkiem określonym w lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

Podstawą powierzenia danych osobowych jest umowa, co do której wymagania zostaną istotnie zmodyfikowane na podstawie przepisów RODO. Jednocześnie RODO dopuszcza też inne instrumenty prawne, które będą wiązały administratora i procesora podległością na terenie UE.

Jednym z obligatoryjnych obowiązków procesora wynikającym z art. 30 ust. 2 RODO jest prowadzenie rejestru wszystkich kategorii czynności przetwarzania danych, które wykonuje w imieniu administratora danych.

RODO nakłada na procesora obwiązek prowadzenia rejestru niezależnie od administratora. Każdy administrator lub podmiot przetwarzający udostępnia rejestr na żądanie organu nadzorczego.

Jednocześnie treść art. 30 ust. 5 RODO wskazuje, iż obowiązku prowadzenia rejestru nie stosuje się do przedsiębiorcy lub podmiotów, które zatrudniają mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

2.4. Formalnoprawne uwarunkowania w zakresie Cloud computing (chmura obliczeniowa)

Ustawa o ochronie danych osobowych zobowiązuje administratora danych do dbałości o bezpieczeństwo danych osobowych, a przepisy rozdziału 5 określają ogólne zasady ich zabezpieczania. Zgodnie z art. 36 ust. 1[lxxiv] tej ustawy, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Wybór odpowiednich środków gwarantujących przetwarzanym danym optymalny stopień zabezpieczenia pozostawia się jednak do decyzji administratorowi danych osobowych. Obowiązki te nie ulegają w żadnym stopniu ograniczeniom w związku z wybranym modelem przetwarzania - cloud computing.

Zarówno przepisy UODO jak i RODO regulują i dopuszczają powierzenie danych osobowych. Należy się tymi przepisami kierować, kształtując umowy w zakresie przetwarzania danych w chmurze obliczeniowej niezależnie od wyboru rozwiązania (chmura prywatna, publiczna, hybrydowa).
Komisja Europejska w motywie 81 preambuły RODO wskazuje na konieczność korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby, odpowiadających wymaganiom bezpieczeństwa przetwarzania, w tym wymaganiom określonym przez RODO.
Stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora. Przetwarzanie przez podmiot przetwarzający powinno być regulowane umową lub innym instrumentem prawnym, które podlegają prawu Unii lub prawu państwa członkowskiego, wiążą podmiot przetwarzający z administratorem, określają przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz które powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Administrator i podmiot przetwarzający mogą postanowić skorzystać z umowy indywidualnej lub ze standardowych klauzul umownych, które zostały przyjęte bezpośrednio przez KE albo które zostały przyjęte przez organ nadzorczy zgodnie z mechanizmem spójności, a następnie przyjęte przez KE.
Po zakończeniu przetwarzania danych podmiot przetwarzający powinien – zgodnie z decyzją administratora – zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania danych osobowych.
Dla zachowania zgodności z RODO, zarówno administrator jak i podmiot przetwarzający powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni. Każdy administrator i każdy

podmiot przetwarzający powinien współpracować z organem nadzorczym i na jego żądanie udostępniać mu te rejestry w celu monitorowania operacji przetwarzania.
W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z RODO zarówno administrator jak i podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak np. szyfrowanie – minimalizujące to ryzyko. Stosowane środki powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

Podkreślenia wymaga, iż w sytuacji gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy dokonać oceny skutków niewłaściwej ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. W celu skutecznego dokonania oceny ryzyka niezmiernie ważne jest uzyskanie wiedzy o lokalizacji danych w chmurze na co wskazuje w swojej opinii Grupa Robocza art. 29 jak i GIODO[14][15].
Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z obowiązującymi w tym zakresie przepisami. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym.
Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

Grupa Robocza art. 29 w opinii 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej przyjętej w dniu 1 lipca 2012 r. przeanalizowała wszystkie kwestie istotne dla dostawców usług przetwarzania danych w chmurze działających w Europejskim Obszarze Gospodarczym (EOG) oraz ich klientów, określając wszystkie mające zastosowanie zasady z Dyrektywy o ochronie danych UE (95/46/WE) oraz Dyrektywy o prywatności i łączności elektronicznej 2002/58/WE (zrewidowanej dyrektywą 2009/136/WE).

[14] Opinia 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej (WP 196), Grupa Robocza art. 29, 2012 r.
[15] Dekalog chmuroluba http://giodo.gov.pl/259/id_art/6271/j/pl

Z oczywistych względów opinia Grupy Roboczej art. 29 nie obejmuje rewizji Dyrektywy 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) natomiast po jego przeanalizowaniu należy stwierdzić, że w tym zakresie nie zachodzą żadne zmiany.
W kolejnym podrozdziale przedstawiono zagrożenia oraz wytyczne w zakresie korzystania z chmury obliczeniowej wskazane przez Grupę Roboczą art. 29, a także zasady stosowania usług chmurowych przez administrację publiczną wydane przez GIODO.

2.4.1. Zagrożenia dla ochrony danych związane z przetwarzaniem danych w chmurze

Grupa Robocza art. 29 w opinii 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej przyjętej w dniu 1 lipca 2012 r. koncentruje się na operacjach przetwarzania danych osobowych, ponadto rozważono w niej tylko określone zagrożenia związane z tym kontekstem. Większość opisanych zagrożeń zalicza się do dwóch kategorii, a mianowicie są to brak kontroli nad danymi oraz niewystarczające informacje dotyczące samej operacji przetwarzania (brak przejrzystości). Szczególne zagrożenia związane z cloud computingiem rozważane w ww. opinii obejmują:

Brak kontroli

Przekazując dane osobowe do systemów zarządzanych przez dostawcę usługi w chmurze, klienci tej usługi mogą nie mieć dalszej wyłącznej kontroli nad swoimi danymi. Oznacza to, że mogą nie mieć możliwości zastosowania środków technicznych i organizacyjnych na przykład w celu zapewnienia dostępności, integralności, poufności, przejrzystości, odizolowania, możliwości interwencji i możliwości przenoszenia danych. Brak zastosowania dostatecznych mechanizmów bezpieczeństwa związanych z procesem transmisji danych do chmury, stwarza ryzyko powstania incydentu umożliwiającego nieuprawnione przejęcie danych, skierowania na niewłaściwy serwer. Ten brak kontroli może przejawiać się w następujący sposób:

- Brak dostępności ze względu na brak interoperacyjności (uzależnienie od dostawcy, tzw. „vendor lock-in"): jeżeli dostawca usługi w chmurze bazuje na zastrzeżonej technologii, dla klienta usługi może się okazać trudne przenoszenie danych i dokumentów między różnymi systemami opartymi na cloud computingu (możliwość przenoszenia danych) lub wymiana informacji z podmiotami korzystającymi z usług w chmurze zarządzanych przez innych dostawców (interoperacyjność).
- Brak integralności spowodowany przez dzielenie się zasobami: chmura składa się z współdzielonych systemów i infrastruktur. Dostawcy usług w chmurze przetwarzają dane osobowe wywodzące się z szeregu licznych źródeł - osób, których dane dotyczą, i organizacji – w związku z tym istnieje prawdopodobieństwo, że mogą powstać sprzeczne interesy i/lub różne cele.
- Brak poufności w odniesieniu do wniosków z zakresu egzekwowania prawa (np. wniosków policji o ściganie, wniosków organów w zakresie prowadzonych czynności dochodzeniowych,

wniosków sądów) składanych bezpośrednio do dostawcy usługi w chmurze, przez organy uprawnione. Istnieje zagrożenie, że dane osobowe mogłyby być ujawnione podmiotom bez podstawy prawnej i tym samym doszłoby do naruszenia prawa dotyczącego ochrony danych. Jak również brak poufności w odniesieniu do technicznej możliwości wglądu do danych dostawców usług.

- Brak możliwości interwencji ze względu na złożoność i dynamiczność łańcucha outsourcingu: usługa w chmurze oferowana przez jednego dostawcę może być realizowana poprzez połączenie usług od szeregu innych dostawców, które mogą być dynamicznie dodawane lub usuwane w czasie trwania umowy klienta.
- Brak możliwości interwencji (prawa osób, których dane dotyczą): dostawca usługi w chmurze może nie zapewnić niezbędnych środków i narzędzi mających pomóc administratorowi zarządzać danymi np. w zakresie dostępu, usunięcia lub poprawienia danych.
- Brak odizolowania: dostawca usługi w chmurze może wykorzystywać swoją fizyczną kontrolę nad danymi od różnych klientów w celu łączenia danych. Jeżeli dostawcy usługi administrujący przetwarzaniem mieliby wystarczające prawa uprzywilejowanego dostępu (role wysokiego ryzyka), mogliby łączyć informacje od różnych klientów (administratorów danych).

Brak informacji na temat przetwarzania (przejrzystości)

Niewystarczające informacje na temat operacji przetwarzania w chmurze stanowi zagrożenie dla administratorów, jak i dla osób, których dane dotyczą, ponieważ mogą oni nie być świadomi potencjalnych zagrożeń i tym samym nie mogą podjąć środków, które uważają za odpowiednie.

Niektóre potencjalne zagrożenia mogą wyniknąć z okoliczności, że administrator może nie być świadomy faktu, że:

- W przetwarzanie zaangażowani są liczni przetwarzający i podprzetwarzający (łańcuch przetwarzania).
- Dane osobowe są przetwarzane w różnych lokalizacjach geograficznych w ramach EOG. Ma to bezpośredni wpływ na prawo właściwe dla ewentualnych sporów z zakresu ochrony danych, które mogą wyniknąć między klientem a dostawcą.
- Dane osobowe są przekazywane do krajów trzecich poza EOG. Kraje trzecie mogą nie zapewniać odpowiedniego poziomu ochrony danych, a operacje przekazywania mogą nie być zabezpieczone odpowiednimi środkami (np. odpowiednie klauzule umowne lub wiążące reguły korporacyjne) i tym samym mogą być niezgodne z prawem obowiązującym klienta.

Wymagane jest poinformowanie osób, których dane osobowe są przetwarzane w chmurze, o tożsamości administratora danych i jego danych kontaktowych oraz, gdy ma to zastosowanie, o tożsamości i danych kontaktowych jego przedstawiciela i celu przetwarzania (istniejący wymóg dla wszystkich administratorów na mocy dyrektywy 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). Zważywszy na potencjalną złożoność łańcuchów przetwarzania

w środowisku przetwarzania w chmurze, w celu zagwarantowania rzetelnego przetwarzania w odniesieniu do osoby, której dane dotyczą (artykuł 10[lxxv] dyrektywy 95/46/WE oraz art. 13 i 14[lxxvi] RODO), administratorzy powinni również, w ramach stosowania dobrych praktyk, zapewnić dalsze informacje dotyczące podprzetwarzających świadczących usługi w chmurze takie jak. np. cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania, informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją, czy też gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych.

2.4.2. Wnioski i zalecenia wydane przez Grupę Roboczą art. 29

Podmioty prywatne oraz podmioty publiczne, które chcą skorzystać z usług przetwarzania danych w chmurze, powinny w pierwszej kolejności przeprowadzić szczegółową analizę zagrożeń. Analiza powinna obejmować zagrożenia związane z przetwarzaniem danych w chmurze, zważając na rodzaj danych przetwarzanych w chmurze. Szczególną uwagę należy zwrócić na oszacowanie zagrożeń dotyczących bezpieczeństwa, w tym z uwzględnieniem dodatkowych zabezpieczeń, a regulowanych przez przepisy właściwe dla ochrony danych osobowych.

Wytyczne dla klientów i dostawców usług przetwarzania danych w chmurze

a) **Relacja administrator-przetwarzający:**
Opinia Grupy Roboczej art. 29 koncentruje się na relacji klient-dostawca jako relacji administrator-przetwarzający. Niemniej, konkretne okoliczności wskazują, że mogą istnieć sytuacje, gdy dostawca usługi w chmurze również działa jako administrator, np. gdy dostawca ponownie przetwarza dane osobowe do własnych celów. W takim przypadku dostawca usługi w chmurze ponosi pełną (wspólną) odpowiedzialność za przetwarzanie i musi spełnić wymagania określone w dyrektywie 95/46/WE a od maja 2018 w RODO.

b) **Odpowiedzialność klienta usługi w chmurze jako administratora:**

Klient jako administrator musi przyjąć odpowiedzialność za przestrzeganie przepisów w zakresie ochrony danych i podlega wszystkim zobowiązaniom prawnym wskazanym w dyrektywie 95/46/WE i 2002/58/WE, gdy to właściwe, w szczególności względem osób, których dane dotyczą . Klient powinien wybrać dostawcę usługi w chmurze, który gwarantuje wykonanie usługi zgodnie z przepisami w zakresie ochrony danych oraz zawrzeć umowę powierzenia, której postanowienia będą odpowiednio zabezpieczały interesy klienta, a także osób których dane osobowe będą przetwarzane.

c) **Zabezpieczenia w przypadku powierzenia:**

Umowa pomiędzy dostawcą usługi a klientem powinna przewidywać postanowienia związane ewentualnym podpowierzeniem realizacji usługi chmurowej. Umowa powinna stanowić, że podprzetwarzającym można powierzyć realizację usług tylko na podstawie zgody udzielonej przez administratora, zgodnie z wyraźnym obowiązkiem przetwarzającego do informowania

administratora o wszelkich planowanych zmianach w tym względzie, przy czym administrator powinien być uprawniony do wyrażenia sprzeciwu wobec takich zmian lub rozwiązania umowy. Należy zobowiązać dostawcę usługi w chmurze do wskazania wszystkich podmiotów, którym podpowierzono usługi. Dostawca usługi w chmurze powinien zostać zobowiązany do zawarcia odrębnej umowy z każdym takim podmiotem, której postanowienia będą umożliwiały dostawcy wywiązanie się z zobowiązań wynikających z umowy zawartej z klientem. Klient powinien zagwarantować sobie w umowie możliwość dochodzenia roszczeń od dostawcy w przypadku naruszenia jej postanowień przez podmioty, którym dostawca podpowierzył usługi.

d) **Przestrzeganie podstawowych zasad ochrony danych:**

Przejrzystość dostawcy usług w chmurze powinna być realizowana poprzez informowanie klientów tych usług o wszystkich istotnych aspektach (dotyczących ochrony danych) odnoszących się do ich usług podczas negocjacji umowy. W szczególności klientów należy poinformować o wszystkich podmiotach, którym podpowierzono realizację usługi i którzy przyczyniają się do świadczenia określonej usługi w chmurze oraz o wszystkich lokalizacjach, w których dane mogą być przetwarzane przez dostawcę usługi w chmurze lub podmioty, którym dostawca podpowierzył usługi (szczególnie gdy niektóre lub wszystkie lokalizacje znajdują się poza EOG). Klientowi należy zapewnić zrozumiałe informacje na temat środków technicznych i organizacyjnych wdrożonych przez dostawcę. Klient w ramach dobrych praktyk, powinien przekazać osobom, których dane dotyczą, informacje na temat dostawcy usługi w chmurze i wszystkich podmiotów, którym dostawca podpowierzył jej realizację (o ile takie podmioty istnieją), jak również na temat lokalizacji, w których dane mogą być przetwarzane przez dostawcę usługi lub podmioty, którym dostawca podpowierzył realizację usług.

e) **Określenie i ograniczenie celu:**

Klient powinien zapewnić zgodność z zasadami określenia i ograniczenia celu oraz zadbać o to, aby żadne dane nie były przetwarzane do innych celów przez dostawcę, podmioty, którym podpowierzył realizację usługi. Zobowiązania w tym zakresie powinny zostać uregulowane w umowie zawartej pomiędzy klientem a dostawcą (w tym zabezpieczenia techniczne i organizacyjne).

f) **Zatrzymywanie danych:**

Klient jest odpowiedzialny za zapewnienie, aby dane osobowe zostały usunięte (przez dostawcę i wszystkie podmioty, którym podpowierzył usługi) ze wszystkich miejsc, w których są przechowywane, jak tylko nie będą już niezbędne do określonych celów. Umowa powinna wskazywać bezpieczne mechanizmy usuwania (zniszczenie, rozmagnetyzowanie, nadpisanie).

g) **Zabezpieczenia umowne:**

Ogólnie: umowa z dostawcą (oraz umowy, które mają być zawarte pomiędzy dostawcą a podmiotami, którym podpowierzono realizację usług) powinna:

i. zapewniać wystarczające gwarancje pod względem zastosowania technicznych środków bezpieczeństwa i środków organizacyjnych (na mocy art. 17 ust. 2[lxxvii] Dyrektywa 95/46/WE) ,
ii. być sporządzona na piśmie,
iii. przedstawiać wiążące instrukcje/wskazówki klienta dla dostawcy, w tym przedmiot i ramy czasowe usługi, cel i wymierne poziomy usługi oraz właściwe sankcje (finansowe lub inne) w przypadku naruszenia jej postanowień,
iv. określać środki bezpieczeństwa, które należy zapewnić stosownie do zagrożeń przetwarzania oraz charakteru danych, zgodnie z wymaganiami wskazanymi poniżej oraz z bardziej rygorystycznymi środkami przewidzianymi w prawie krajowym klienta,
v. przewidywać, że w sytuacji gdy dostawcy usług w chmurze dążą do wykorzystania standardowych klauzul umownych o których mowa w ust. 7 i 8 art. 28 RODO, także gdy są one elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43 RODO, powinni oni zapewnić, że postanowienia te będą zgodne z wymaganiami w zakresie ochrony danych, w szczególności należy określić środki techniczne i organizacyjne wprowadzone przez dostawcę.

h) **Dostęp do danych**:

Tylko upoważnione osoby powinny mieć dostęp do danych; w umowie powinna być przewidziana klauzula poufności dla dostawcy, którego odpowiedzialność za dochowanie poufności będzie obejmowała również jego pracowników.

i) **Udostępnianie danych osobom trzecim:**

Zagadnienia związane z udostępnianiem danych osobom trzecim powinno zostać uregulowane w umowie. Dostawca powinien zostać zobowiązany do wskazania wszystkich podmiotów, którym podpowierzył realizację usługi – np. w publicznym rejestrze cyfrowym – oraz do zapewnienia klientowi dostępu do informacji o wszelkich zmianach w celu umożliwienia mu wyrażenia sprzeciwu wobec tych zmian lub do rozwiązania umowy. Umowa powinna również przewidywać zobowiązanie dostawcy do zgłaszania wszelkich prawnie wiążących wniosków o udostępnienie danych osobowych przez organ egzekwowania prawa, o ile takie udostępnienie nie jest zakazane w inny sposób Dostawca powinien zostać zobowiązany do odrzucenia wniosków o udostępnienie, które będą nieuprawnione.

j) **Zobowiązania do współpracy:**

Dostawca powinien zostać zobowiązany do współpracy w związku z prawem klienta do monitorowania operacji przetwarzania, do ułatwiania realizacji praw osób, których dane dotyczą, do dostępu do/poprawiania/usuwania ich danych, oraz (gdy to właściwe) do

powiadamiania klienta usługi w chmurze o wszelkich naruszeniach ochrony danych mających wpływ na dane klienta.

k) **Transgraniczne przekazywanie danych:**

Klient usługi w chmurze powinien zweryfikować, czy dostawca usługi w chmurze może zagwarantować legalność transgranicznego przekazywania danych oraz ograniczyć przypadki przekazywania do krajów wybranych przez klienta, gdy to możliwe. Przekazywanie danych do krajów trzecich niezapewniających odpowiedniego poziomu ochrony wymaga szczególnych zabezpieczeń przy wykorzystaniu odpowiednio zobowiązań umownych 'EU-US-Privacy Shield'. Dla przetwarzających wymaga to pewnych dostosowań do środowiska cloud computingu (aby zapobiec temu, że będą istniały odrębne umowy dla danego klienta między dostawcą i podmiotami, którym podpowierzył usługi), co może oznaczać potrzebę wcześniejszej autoryzacji zgodności z wymogami przez właściwy organ ochrony danych; lista lokalizacji, w których może być świadczona usługa powinna być zawarta w umowie.

l) **Rejestrowanie (ang. „logging") i kontrolowanie przetwarzania:**

Klient powinien wymagać rejestrowania operacji przetwarzania dokonywanych przez dostawcę lub podmioty, którym podpowierzył realizację usług; klient powinien być uprawniony do kontroli (audytu) takich operacji przetwarzania, jednak kontrole dokonywane przez osoby trzecie wybrane przez administratora oraz certyfikacja również mogą być dopuszczalne, pod warunkiem że zagwarantowana jest pełna przejrzystość (np. poprzez zapewnienie możliwości uzyskania kopii certyfikatu potwierdzającego kontrolę dokonaną przez osobę trzecią lub kopii sprawozdania z kontroli weryfikującej certyfikację).

m) **Środki techniczne i organizacyjne:**

Powinny mieć na celu eliminację lub złagodzenie zagrożeń wynikających z braku kontroli i braku informacji, które najczęściej charakteryzują środowisko cloud computingu. Chodzi tu o środki mające na celu zapewnienie dostępności, integralności, poufności, odizolowania, możliwości interwencji i przenoszenia danych, jak określono w dokumencie, podczas gdy środki skupiają się na przejrzystości.

n) **Certyfikacja w zakresie ochrony danych zapewniana przez strony trzecie:**

Niezależna weryfikacja i certyfikacja przez renomowaną w tym zakresie osobę trzecią może być dla dostawców usług w chmurze wiarygodnym sposobem wykazania, że przestrzegają zobowiązań określonych w Opinii GR. Taka certyfikacja wskazywałaby co najmniej, że kontrole w zakresie ochrony danych zostały poddane audytowi lub przeglądowi zgodnie z uznanym standardem spełniającym wymogi określone w Opinii GR. W kontekście cloud computingu potencjalni klienci powinni zweryfikować, czy dostawcy usług w chmurze mogą zapewnić kopie

takiego certyfikatu potwierdzającego kontrolę dokonaną przez osobę trzecią lub kopię sprawozdania z kontroli weryfikującej certyfikację, w tym w odniesieniu do wymogów określonych w Opinii GR.

Niezależne kontrole danych utrzymywanych na wirtualnych serwerach (hosting) przeznaczonych dla wielu stron mogą być niepraktyczne pod względem technicznym i mogą w niektórych przypadkach prowadzić do zwiększenia zagrożeń dla istniejących kontroli bezpieczeństwa fizycznego i logicznego sieci. W takich przypadkach kontrola wykonywana przez osobę trzecią wybraną przez administratora może być uznana za wystarczającą realizację prawa danego administratora do kontroli.

o) **Przyjęcie standardów i certyfikacji typowych dla ochrony prywatności**

Przyjęcie standardów i certyfikacji typowych dla ochrony prywatności jest szczególnie istotne dla ustanowienia wiarygodnej relacji między dostawcami usług w chmurze, administratorami i osobami, których dane dotyczą.

Standardy i certyfikacje powinny dotyczyć środków technicznych (takich jak lokalizacja danych lub szyfrowanie) oraz procesów w środowisku dostawców usług w chmurze, które gwarantują ochronę danych (takich jak polityki kontroli dostępu, kontrola dostępu lub kopie zapasowe).

2.4.3. Zasady korzystania z usług chmurowych przez administrację publiczną wg GIODO

GIODO opublikował w 2013 roku dokument pod nazwą „Dekalog chmuroluba", poświęcony zasadom korzystania z chmury obliczeniowej przez administrację publiczną. Jednocześnie GIODO zastrzega, że „nie jest to oficjalny dokument będący docelowym zestawem wskazań dla użytkowników chmury"[16]. Ze względu na fakt, że od czasu opublikowania dokumentu minęło kilka lat i w tym czasie nastąpił postęp technologii oraz doszło do zmian przepisów prawa zarówno na poziomie krajowym jak i UE, zawarte w dekalogu zasady należy interpretować z uwzględnieniem obecnych uwarunkowań.

Podsumowanie

Każdy usługodawca ma możliwość wyboru dowolnego rozwiązania chmurowego. Decydując się na wybór określonej usługi usługodawca musi uwzględnić wymagania wynikające z przepisów prawa.

2.4.4. Standardy ochrony danych osobowych w usługach chmurowych

Międzynarodowe standardy ochrony danych osobowych mają na celu zapewnienie najbardziej możliwej ochrony istotnych danych osobowych w tym danych o stanie zdrowia i konsekwentne minimalizowanie ryzyka związanego z ich przetwarzaniem.

[16] http://giodo.gov.pl/259/id_art/6271/j/pl

Niezależnie od wymagań prawnych, podstawowymi standardami postępowania z danymi osobowymi są powszechnie stosowane normy takie jak: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 22301, ISO/IEC 27018 czy ISO 10781:2015. Normy te stanowią istotną wskazówkę przy wyborze dostawców rozwiązań IT.

Norma ISO/IEC 27001 dotyczy zarządzania bezpieczeństwem informacji. Odnosi się m.in. do takich kwestii jak polityka bezpieczeństwa, organizacja bezpieczeństwa informacji, zarządzanie ciągłością działania czy zgodność z wymaganiami prawnymi. Europejski Komitet Ekonomiczno-Społeczny wskazał na konieczność wdrożenia normy ISO 27001 na szczeblu międzynarodowym w celu zapewnienia bezpieczeństwa danych przetwarzanych w ramach tzw. m-zdrowia.

Norma ISO/IEC 27002 wyznacza zasady ustanowienia, wdrażania, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji. Rozwija merytorycznie wytyczne, które zawarte są w normie ISO/IEC 27001.

Norma ISO/IEC 22301 wyznacza zasady zarządzania zagrożeniami dla działalności z punktu widzenia jej ciągłości biznesowej. Wyznacza ona wymagania stawiane systemom zarządzania mającym zapobiec niespodziewanym incydentom zakłócającym ich pracę. Dzięki wdrożeniu systemu dochodzi do zmniejszenia prawdopodobieństwa wystąpienia tego typu incydentów i zapewnienia, że nawet w przypadku dojścia do nich, zostanie utrzymana ciągłość działalności.

Norma ISO/IEC 27018 stosowana jest w połączeniu z normą ISO/IEC 27001 i podobnie jako ona odnosi się do procesu zarządzania bezpieczeństwem informacji. Konkretyzuje standardy dotyczące bezpiecznego wykorzystywania publicznej chmury obliczeniowej.

Do procesu przetwarzania danych o stanie zdrowia w systemach IT odnosi się także kilka norm branżowych (sektorowych), do których można zaliczyć ISO 27799, Informatyka w ochronie zdrowia – Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002, ISO 13606-1, Informatyka w ochronie zdrowia – Przesyłanie elektronicznej dokumentacji zdrowotnej – Część 1: Model referencyjny oraz ISO 13606-4, Informatyka w ochronie zdrowia – Przesyłanie elektronicznej dokumentacji zdrowotnej – Część 4: Bezpieczeństwo danych.

Norma ISO/IEC 27018 nawiązuje pod względem merytorycznym bezpośrednio do normy ISO/IEC 27002. ISO 27018 specyfikuje działania bezpieczeństwa (controls) w następujący sposób: istnieje możliwość integracji szczególnych wymagań ochrony danych osobowych w ramach usług przetwarzania danych w chmurze w istniejący system zarządzania bezpieczeństwa informacji. Zawartość normy ISO 27002 w ISO 27018 jest poszerzona o aspekty danych w chmurze. ISO 27018 spełnia swoimi wymaganiami w dużej mierze projekt zaplanowanego Rozporządzenia UE dotyczący ochrony danych, jak i austriacką i niemiecką ustawę o ochronie danych. Dlatego też większość przedsiębiorstw definiuje w ramach projektu certyfikacji według ISO 27018, które państwowe wymagania prawne są istotne dla ich oferowanych usług w obrębie „chmury” oraz istotne dla ich klientów i partnerów. Słownictwo i zawartość ISO/IEC 27018 kieruje się normą ISO/IEC 17788 „Cloudcomputing – overview and vocabular” oraz ISO/IEC 29100 „Privacyframework”.

Główne wymagania ISO 27018 względem usługodawców „chmury”:

a) Dane osobowe mogą być przetwarzane tylko i wyłącznie za wyrażeniem zgody przez klienta oraz wyłącznie do celów nieosobistych, oprócz sytuacji wyrażenia zgody przez klienta na tego rodzaju działanie.
b) Należy zdefiniować procesy określające: zwrot, przekazanie, zniszczenie danych osobowych.
c) Przed zakończeniem umowy należy ujawnić wszelkie podzlecenia usług przetwarzania oraz wszystkie kraje, w których występuje przetwarzanie danych.
d) Każdego rodzaju naruszenie ochrony danych należy udokumentować – łącznie z ustalonymi krokami rozwiązywania problemów i możliwymi następstwami.
e) Naruszenie ochrony danych należy niezwłocznie zgłosić klientowi!
f) Należy wspierać klientów w zakresie postrzegania swoich praw: klientom, których dane przetwarzane są w chmurze należy oferować narzędzia, pozwalające by końcowi użytkownicy mogli uzyskać dostęp do swoich danych osobowych, w celu ich zmiany, usunięcia lub korekcji.
g) Przekazanie danych osobowych organom ścigania może nastąpić tylko i wyłącznie w przypadku istnienia prawnych zobowiązań w tym zakresie. Należy poinformować klienta, objętego takim postępowaniem, o ile informacja ta nie została utajniona.
h) Oferowane usługi ‘danych w chmurze’ należy poddać regularnym kontrolom przez osoby trzecie.

Podsumowanie

Usługi chmurowe certyfikowane na zgodność z normą ISO/IEC 27018:2014 stanowią podstawę domniemania , że podmioty świadczące te usługi zapewniają odpowiedni poziom bezpieczeństwa.

Część III. Zagrożenia i odpowiedzialność wynikająca z przetwarzania dokumentacji medycznej w postaci elektronicznej

1. Zagrożenia występujące podczas przetwarzania dokumentacji medycznej w postaci elektronicznej

Naruszenie podstawowych atrybutów bezpieczeństwa przetwarzania informacji tj. naruszenie poufności, integralności i dostępności danych medycznych obejmuje poniższe zagrożenia[17]:

a) Nieuprawniony dostęp przez użytkowników (w tym nieuprawniony dostęp przez pracowników służby zdrowia i personelu pomocniczego) polegający na zaistnieniu sytuacji, w której użytkownicy korzystają z kont do których sami nie mają uprawnień albo korzystania przez wielu użytkowników z tego samego loginu użytkownika i hasła. „Pragmatyzm zwyczajowy" stanowi naruszenie zasad bezpiecznego uwierzytelniania użytkownika. Przykładem takiego zwyczaju mogą być sytuacje w których jeden pracownik medyczny (np. lekarz) może zastąpić innego na stanowisku pracy i kontynuuje prace na już zalogowanym koncie poprzednika co skutkuje brakiem potrzeby przelogowania. Pierwsze logowanie użytkownika pozwala na pracę w systemie i jednocześnie bez uprzedniego wylogowania pozwala na pracę przez innych użytkowników na koncie bieżącego użytkownika. Powyższy przykład zachowania powoduje poważne naruszenia poufności i niezaprzeczalności. Większość naruszeń poufności jest dokonywana przez użytkowników pracujących w danej organizacji a genezą ich powstania są uwarunkowania spowodowane w znacznym zakresie brakiem świadomości użytkowników o zagrożeniach z nich wynikających. W tym miejscu wskazać również należy, że nieuprawniony dostęp przez użytkowników może służyć do próby zatuszowania przypadków lub przypisania zdarzeń innej osobie, gdy zdarzenia takie powstały. Dlatego też funkcjonalności użytkowanych systemów informatycznych powinny pozwalać wyeksportować pełen wykaz wykonywanych czynności na danych w systemie, zawierający: określenie czasu ich wykonania, reguł wersjonowania (brak możliwości nadpisywania) oraz identyfikację rodzaju dokonanej czynności.
b) Nieuprawniony dostęp przez użytkowników (w tym usługodawcy uprawnieni na podstawie umów - personel obsługi technicznej - administratorzy oprogramowania i sprzętu, którzy mogą mieć uzasadniony powód dostępu do systemów i danych) posiadających uprzywilejowany dostęp do systemów i urządzeń polegający na uzyskaniu nieautoryzowanego dostępu do danych. Działanie takie jest naruszeniem bezpiecznych rozwiązań wynikających z umów outsourcingowych. Nieuprawniony dostęp przez usługodawców może być także źródłem poważnych naruszeń poufności informacji w tym danych medycznych.
c) Nieuprawniony dostęp przez osoby z zewnątrz organizacji - zaistnieje w sytuacji w której nieuprawnione osoby trzecie (hakerzy) posiadają dostęp do danych lub zasobów

[17] PN-EN ISO 27799:2016 Informatyka w ochronie zdrowia -- Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002

systemowych, albo poprzez podszywanie się jako autoryzowany użytkownik stanie się upoważnionym użytkownikiem (na przykład przez tak zwany atak wykorzystujący metody socjotechniczne). Oprócz hakerów osobami trzecimi mogą być np.. dziennikarze, prywatni detektywi i "haktywiści" (hakerzy, którzy działają w imieniu lub w sympatii, politycznych grup nacisku). Przypadek nieuprawnionego dostępu przez użytkowników z zewnątrz może świadczyć o pominięciu kontroli bezpieczeństwa w zakresie:

- identyfikacji użytkownika;
- uwierzytelniania użytkownika;
- identyfikacji użytkownika z uwierzytelnieniem zaufanego sprzętu;
- uwierzytelniania pochodzenia;
- kontroli dostępu i zarządzania uprawnieniami.

d) Nieuprawnione wykorzystanie aplikacji przetwarzającej informacje na temat zdrowia pacjentów skutkujące możliwością uzyskania nieautoryzowanego dostępu do aplikacji informatycznych systemu ochrony zdrowia (np. polegających na dostępie do systemu na niestrzeżonym stanowisku pracy w gabinecie lekarza i przeglądanie na ekranie informacji dotyczących pacjentów). Jednocześnie upoważnieni użytkownicy mogą również dokonywać nieautoryzowanych działań, takich jak celowe zmienianie danych. Krytyczne znaczenie prawidłowej identyfikacji użytkowników i prawidłowego dopasowania ich uprawnień do ich dokumentacji medycznej prowadzi organizacje do zbierania szczegółowych informacji umożliwiających zidentyfikowanie użytkowników dokonujących wglądu w dane medyczne. Z uwagi na potencjalną wartość tych danych (np. w kontekście kradzieży tożsamości) powinny być one ściśle chronione. Należy również pamiętać, że nieuprawnione korzystanie z aplikacji informatycznych systemów ochrony zdrowia stanowi brak jednego lub więcej z następujących zabezpieczeń:

- kontroli dostępu dla grup roboczych (np. poprzez umożliwienie użytkownikowi dostępu do ewidencji z których użytkownik nie ma możliwości legalnego korzystania);
- odpowiedzialności i kontroli sterowania (np. poprzez umożliwienie niewłaściwego działania użytkowników, aby ich działania były niezauważalne);
- bezpieczeństwa pracowników (np. poprzez niezapewnienie wystarczających szkoleń użytkowników);

e) Możliwość uszkodzenia lub wprowadzenia do systemu destrukcyjnego oprogramowania obejmującego np. wirusy, lub inne "złośliwe oprogramowanie"). Większość incydentów bezpieczeństwa IT wiąże się z wprowadzeniem do systemu wirusów komputerowych. Wprowadzenie szkodliwego lub uciążliwego oprogramowania może być spowodowane brakiem ochrony antywirusowej lub kontroli zmian oprogramowania. Podczas procesu ataku na sieć informatyczną i rozprzestrzeniania się wirusów, a także wykorzystywania przez hakerów słabych punktów oprogramowania serwerowego, może dochodzić do maskowania wykonywanych czynności przy jednoczesnym uszkadzaniu lub destrukcji systemu.

f) Nadużywanie zasobów systemowych jest również zagrożeniem dla użytkowników systemów informacyjnych opieki zdrowotnej i usług korzystających z pracy zdalnej. Użytkownicy tacy pobierają informacje, zgodne z charakterem swojej pracy, z Internetu na komputer

przeznaczonych do obsługi systemów informacji zdrowotnej co w dalszej kolejności może skutkować tworzeniem nowych baz danych w systemie. Praca zdalna przez wielu użytkowników może również wpływać na pogarszanie się dostępności systemu informacji, spowodowanym na przykład zmniejszeniem przepustowości. Jednocześnie wskazać należy, że nawiązywanie połączeń streamingu video lub audio w celach prywatnych może powodować nadużycia. Konieczne jest więc edukowanie użytkowników o wpływie i znaczeniu utrzymania integralności i dostępności zasobów informacyjnych opieki zdrowotnej.

g) Infiltracja komunikacji elektronicznej występuje wówczas, gdy nieuprawniony użytkownik (na przykład haker) manipuluje w normalnym przepływie danych w sieci. Najczęstszym atakiem jest atak Denial of Service (w tym serwerów lub zasobów sieciowych będących w trybie off-line), ale możliwe są także inne rodzaje infiltracji komunikacji takie jak atak out-of-date na retransmitowaną wiadomość. Infiltracja komunikacji może utrudniać wykrywanie włamań i / lub utrudniać dostęp do sieci i kontrolę (w szczególności analizę luki) w celu ochrony architektury systemu (który musi być zaprojektowany z myślą o ochronie przed atakami denial-of-service).

h) Przechwycenie komunikacji. W przypadku gdy przekazywanie danych nie następuje w formie zaszyfrowanej (kryptograficzna ochrona transmisji danych) podczas ich przesyłania, może zaistnieć sytuacja, w której zostaną one przechwycone przez nieuprawnioną osobę. Zagrożenie to jest prostsze, ponieważ każdy pracując w lokalnej sieci może potencjalnie zainstalować tzw. "sniffer pakietów" na swoim stanowisku pracy i monitorować większość ruchu w sieci lokalnej, w tym w trakcie np. transmisji. Narzędzia hakerskie są łatwo dostępne i w pełni zautomatyzowane. Przechwytywanie komunikacji stanowi istotne zagrożenie w bezpieczeństwie komunikacji.

i) Brak niezaprzeczalności to zagrożenie, które stanowi, że podczas przetwarzania informacji dochodzi do jej odrzucenia z powodu braku niezaprzeczalności jej pochodzenia lub niezaprzeczalności użytkownika, który ją wysłał (odrzucenie nadania) lub otrzymał (odrzucenie odbioru). Jednocześnie taki brak jednoznacznego ustalenia czy dane medyczne, przesyłane z jednego do drugiego podmiotu służby zdrowia, rzeczywiście zostały nadane i odebrane może być jedną z istotnych cech śledztw dotyczących błędów lekarskich. Negowanie może stanowić brak zastosowania elementów sterujących, takich jak podpisy elektroniczne na dokumentacji medycznej (przykład odrzucenie pochodzenia) lub sterujące, takie jak wpływ na odczyt wiadomości e-mail (przykład odrzucenie odbioru).

j) Błąd połączenia (w tym awarie sieci informacyjnych zdrowia). Wszystkie sieci są przedmiotem okresowych przerw serwisowych. Jakość usług jest głównym czynnikiem ciągłości usług sieciowych w zakresie opieki zdrowotnej. Błąd połączenia może wynikać z niedostępności usług sieciowych (na przykład złośliwe zmiany tablic routingu, które powodują przekierowanie ruchu sieciowego). Wskazać należy, że awarie połączeń mogą ułatwić ujawnienie poufnych informacji poprzez zmuszanie użytkowników na wysyłanie wiadomości przez połączenie nie zapewniające mechanizmów bezpieczeństwa, na przykład za pośrednictwem faksu lub za pośrednictwem nieszyfrowanego połączenia z sieci publicznej (hot-spot).

k) Osadzanie złośliwego kodu. Zagrożenie to obejmuje wirusy przesyłane w wiadomościach e-mail i wykorzystanie złośliwego kodu mobilnego. Zwiększenie wykorzystania technologii bezprzewodowych i komórkowych przez pracowników służby zdrowia zwiększa potencjał tego zagrożenia. Osadzanie złośliwego kodu stanowi brak skutecznego stosowania kontroli oprogramowania antywirusowego lub kontroli zapobiegania włamaniom.

l) Przekierowanie połączenia. Zagrożenie to obejmuje możliwość, że informacje przesyłane przez sieć informatyczną mogą być dostarczone do niewłaściwego adresata. Przypadkowe przekierowanie połączenia może stanowić uchybienie w działaniu systemu lub niemożność utrzymania integralności informacji przetwarzanych w dokumentacji medycznej.

m) Awaria techniczna systemu lub infrastruktury sieciowej. Zagrożenia te obejmują awarie sprzętu, awarie sieci lub braki w bazach danych. Takie problemy zwykle stanowią o awarii jednego lub większej liczby elementów powodując jego ograniczone działanie lub niedostępność. Utrata dostępności takich systemów może mieć zagrażające życiu skutki dla pacjentów.

n) Awaria środowiska wsparcia w tym awarie zasilania i zakłócenia wynikające z oddziaływania fizycznego lub katastrof spowodowanych przez człowieka. Systemy informacji zdrowotnej mogą być systemami krytycznymi, których naruszenie ciągłości działania podczas klęsk żywiołowych i innych zdarzeń może stanowić zagrożenie życia ludzi. Te same katastrofy mogą jednak spowodować duże zniszczenia w systemach wsparcia środowisk niezbędnych do utrzymania działalności. Właściwa ocena zagrożenia i ryzyka informacji na temat zdrowia będzie zawierać wnioski, jak krytyczne są systemy funkcjonujące podczas klęski żywiołowej i jaka będzie ich ciągłość działania.

o) Awaria systemu lub oprogramowania sieciowego. Ataki DoS są znacznie ułatwione dzięki słabościom lub błędom systemu operacyjnego lub oprogramowaniu sieciowemu. Awaria systemu lub sieci może być spowodowana awarią oprogramowania do sprawdzania integralności i testowania systemu kontroli lub konserwacji oprogramowania.

p) Awaria oprogramowania aplikacji. Błędy w oprogramowaniu aplikacyjnym mogą zostać wykorzystane na atak Denial of Service oraz mogą być również powodem utraty poufności danych chronionych. Awaria aplikacji stanowi awarię w testowaniu oprogramowania, kontroli zmian oprogramowania lub sprawdzania integralności oprogramowania.

q) Błędne operacje. Błędy operatora odpowiadają za niewielki, ale znaczący procent niezamierzonych ujawnień poufnych informacji w tym tych dotyczących stanu zdrowia pacjentów. Błędy operatora stanowią o braku jednego lub więcej czynników takich jak:
   - kontrola operacji;
   - bezpieczeństwo personelu (w tym brak skutecznego szkolenia).

r) Odzyskiwanie po awarii (w tym tworzenia kopii zapasowych i przywracania systemów).

s) Błąd konserwacji. Błędy konserwacji są błędami wywoływanymi przez osoby odpowiedzialne za utrzymanie systemów, sprzętu i oprogramowania. Błędy konserwacyjne mogą być popełniane zarówno przez pracowników jak również przez osobę trzecią. Błędy te mogą jednocześnie zagrażać poufności chronionych danych. Rekonfiguracja oprogramowania podczas instalacji jest przyczyną luki, która później może zostać wykorzystana przez osoby

trzecie. Błędy w konserwacji mogą skutkować awarię oprogramowania sterującego, zmianą tego oprogramowania oraz mogą być kombinacją powyższych.

t) Błąd użytkownika. Błędy generowane przez użytkowników mogą na przykład prowadzić do przesłania poufnych informacji do niewłaściwego odbiorcy. Błędy użytkownika mogą czasami stanowić uchybienie w:
   - kontroli użytkownika (włącznie z interfejsami użytkownika zaprojektowanymi z myślą o bezpieczeństwie)
   - bezpieczeństwu personelu (w tym podnoszenie świadomości i zapewnieniu dostępu do informacji i realizowaniu procesu szkolenia).

   Błędne udostepnienie danych osobom nieuprawnionym skutkujące brakiem możliwości odwołania lub cofnięcia przesłanych danych powoduje w dalszej kolejności brak kontroli w ich dalszej dystrybucji. Wskazać należy, iż komunikaty o niezapoznawaniu się z przesłanymi pomyłkowo danymi wzbudzają dodatkową ciekawość użytkowników, przez co znacząco zwiększa się prawdopodobieństwo, że osoba nieuprawniona zapozna się z tymi danymi.

u) Niedobór personelu. Groźba niedoboru personelu obejmuje możliwość braku kluczowych pracowników jak również braku możliwości ich zastąpienia np. w trakcie urlopu. Podatność na to zagrożenie zależy głównie od tego, w jakim stopniu brak pracowników wpłynie na procesy biznesowe jednostki. W służbie zdrowia, epidemia, która znacznie zwiększa zapotrzebowanie na szybki dostęp do informacji na temat zdrowia może również spowodować niedobory personelu zagrażając dostępności takich systemów. Awaria tego typu stanowi naruszenie ciągłości biznesowej.

v) Kradzież przez użytkowników w tym kradzież sprzętu lub danych. Użytkownicy systemów zazwyczaj mają większy dostęp do informacji poufnych i są w związku z tym podatni na kradzież informacji, aby ją następnie sprzedać lub ujawnić. Zagrożenie kradzieży informacji zawartych w dokumentacji medycznej spowodowane jest chęcią uzyskania korzyści lub sławy oraz rozgłosu i najczęściej może dotyczyć np. osób z pierwszych stron gazet, celebrytów, polityków. Dążenie do nieuprawnionego uzyskania informacji w tym jej upublicznienia maleje jednak wraz z dotkliwością skutków karnych (np. utraty przez lekarza prawa do wykonywania zawodu). Kradzież przez użytkowników stanowi naruszenie jednej z wielu możliwych kontroli, w tym kontroli dokumentów i nośniki informacji, bezpieczeństwa fizycznego lub fizycznej ochrony urządzeń.

w) Kradzież przez osoby z zewnątrz (w tym kradzieży sprzętu lub danych). Kradzież danych i sprzętu przez osoby z zewnątrz jest poważnym problemem w niektórych szpitalach. Kradzież może powodować naruszenia poufności dlatego, że poufne dane są przechowywane na komputerze lub laptopie, który został skradziony albo dlatego, że celem kradzieży były same dane. Kradzież z zewnątrz może stanowić uchybienie w jednej z wielu kontroli, w tym kontroli komputerów mobilnych, kontroli zgodności lub fizycznej ochrony przed kradzieżą.

x) Samowolne uszkodzenia przez użytkowników obejmują akty wandalizmu oraz inne przypadki, w których szkoda fizyczna jest wyrządzona systemom informatycznym lub środowiskom wspieranym przez osoby, które uzyskały do nich dostęp. Użytkownikami systemów informacyjnych ochrony zdrowia są zazwyczaj dedykowani pracownicy służby zdrowia co

powoduje, że przypadki umyślnego uszkodzenia są bardzo rzadkie. Samowolne uszkodzenia przez użytkowników stanowią naruszenie bezpieczeństwa zasobów ludzkich.

y) Samowolne uszkodzenia przez osoby z zewnątrz. Groźba umyślnego uszkodzenia przez osoby z zewnątrz obejmuje zarówno akty wandalizmu oraz inne przypadki, w których fizyczne szkody wyrządzone systemom informatycznym lub środowiskom przez osoby, które nie uzyskały dostępu do tych systemów. Podczas gdy w większości sektorów przemysłowych, awarie tego typu stanowią brak skutecznego zastosowania kontroli bezpieczeństwa fizycznego, to dostęp do systemów informatycznych przez pacjentów i ich krewnych w obszarach operacyjnych szpitali, klinik i innych organizacjach ochrony zdrowia jest dużo łatwiejszy. Kontrole bezpieczeństwa muszą być starannie dobrane i dostosowane w celu minimalizacji tych zagrożeń.

z) Terroryzm. Zagrożenie terroryzmem obejmuje akty realizowane przez grupy ekstremistów, którzy mogą chcieć uszkodzić lub zakłócić pracę organizacji ochrony zdrowia albo zaszkodzić pracownikom służby zdrowia jak również zakłócić działanie systemów informacji zdrowotnej. Chociaż takie ataki nie mają obecnie miejsca, to istnieje uzasadniona potrzeba rozważenia zagrożenia terroryzmem, zwłaszcza gdy systemy informacji zdrowotnej są wielkoskalowe i należą do infrastruktury krytycznej, ponieważ atak na takie systemy może spowodować zaburzenie ich ciągłości działania.

2. Cyberbezpieczeństwo przetwarzania dokumentacji medycznej w postaci elektronicznej

Obecnie utrwaliło się przekonanie, że na ataki cyberprzestępców najbardziej narażone są sektory związane z finansami, energetyką czy transportem. Jednak zauważyć należy, że ostatnio coraz częściej ataki takie skierowane są również na systemy szpitalne czy nawet same urządzenia medyczne, które jak wskazują międzynarodowe instytucje są słabo zabezpieczone. To właśnie w tych systemach przetwarzane są w większości przypadków wrażliwe dane dotyczące zdrowia pacjentów.

Ostatnie doniesienia prasowe wskazują, że blokada systemu informatycznego czy też wyciek danych o pacjentach mogą skutecznie zdezorganizować prace jednostki medycznej w takim stopniu, że nie będzie ona w stanie leczyć pacjentów dopóki np. nie zapłaci wysokiego okupu cyberprzestępcom. Wielokrotnie okazuje się, że pomimo zapłacenia żądanego okupu, system informatyczny w dalszym ciągu był dla jednostki niedostępny, a przetwarzane w nim dane zostały nieodwracalnie zaszyfrowane.

Obecnie dane medyczne są w większości przetwarzane w postaci elektronicznej przy pomocy systemów informatycznych. W tym miejscu wskazać należy, że np. w 2018 roku zaistnieje możliwość wystawiania e-recepty, zaś w 2019 r. obowiązek prowadzenia EDM. Dynamicznie również rozwija się telemedycyna, w ramach której dane diagnostyczne pacjenta mogą być przesyłane, w celu konsultacji, do specjalistów znajdujących się w wielu lokalizacjach. Powstają też różnorodne aplikacje medyczne do samodzielnego używania przez pacjentów. Roboty medyczne wspomagają chirurgów, umożliwiając im przeprowadzanie coraz bardziej skomplikowanych operacji. Nowe rozwiązania Internetu w znacznej części zastępują czynności personelu medycznego, umożliwiając bezpośrednią komunikację pomiędzy urządzeniami medycznymi i automatyczne ustawianie właściwych parametrów, np. dawkowania

pacjentom insuliny. Stało się obecnie jasne, że powodzenie w leczeniu zależy w większym niż kiedykolwiek stopniu właśnie od bezpieczeństwa informatycznego szpitali[18].

Niestety okazało się również, że ciemną stroną skoku technologicznego jest zwiększone ryzyko utraty danych w wyniku działalności cyberprzestępców. Jak pokazują dotychczasowe zdarzenia np. z Wielkiej Brytanii czy USA, scenariusz tzw. ataków ransomowych najczęściej polega na sytuacji w której do pracowników szpitala wysyłana jest seria maili z pozornie legalną treścią (np. zawiadomienie o kongresie naukowym, zaproszenie do udziału w atrakcyjnym projekcie badawczym itd.). Po otwarciu maila w komputerze automatycznie instaluje się nielegalne oprogramowanie (tzw. malware), które skanuje zawartość sieci, do której podłączony jest komputer, a następnie blokuje dostęp do danych pacjentów i przesyła je w zaszyfrowanej formie do komputera, z którego pochodzi atak. W takiej sytuacji wobec utraty danych oraz blokady systemu szpital jest zmuszony do zawieszenia działalności medycznej, a dyrekcja otrzymuje e-mail z żądaniem zapłaty określonej sumy w zamian za zwrot danych oraz odblokowanie systemu.

Szacuje się, że w latach 2017-2021 globalna wartość strat wynikających z działalności cyberprzestępców na świecie wyniesie 6 bilionów USD, a konieczne wydatki związane z zapewnieniem cyberbezpieczeństwa w tym okresie pochłoną co najmniej 1 bilion USD. Tymczasem w szpitalach nadal niska jest świadomość dotycząca skali zagrożenia cyberatakami. Efektem jest brak stosownych procedur wewnętrznych mających na celu ochronę systemów informatycznych, a to z kolei jest bezpośrednią przyczyną niewystarczającego zabezpieczenia wrażliwych danych pacjentów[19].

Opracowanie i wdrożenie przepisów chroniących przed cyberprzestępczością to wieloletni proces wymagający zaangażowania zarówno ustawodawcy europejskiego, jak i krajowego oraz dialogu z podmiotami z różnych sektorów gospodarki, w tym ochrony zdrowia.

Dyrektywa NIS (Dyrektywa Parlamentu i Rady UE 2016/1148[20] w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii przyjęta 6 lipca 2016 roku) zakłada poszerzenie współpracy państw członkowskich w kwestii cyberbezpieczeństwa. Jednym z sektorów objętych dyrektywą jest sektor e-zdrowia zawierający zagadnienia przetwarzania elektronicznej dokumentacji medycznej.

Zgodnie z Dyrektywą NIS konieczne jest zapewnienie przez poszczególne podmioty mające udział w przetwarzaniu EDM minimalnego poziomu ochrony dla infrastruktury w tym sieci i systemów przetwarzających dokumentację medyczną. Poprzez realizację tego wymogu rozumieć należy wdrożenie odpowiednich środków bezpieczeństwa w warstwie organizacyjnej, technicznej i systemowej oraz w przypadku wystąpienia poważnych incydentów bezpieczeństwa informacji podjęcie odpowiednich działań ograniczających ich skutki, a co najważniejsze powiadomienie krajowego organu cyberbezpieczeństwa jakim jest CERT Polska. Krajowy organ będzie mógł nakładać

18 http://www.codozasady.pl/cyberbezpieczenstwo-a-sektor-ochrony-zdrowia

19 Tamże

20 Dyrektywy PE i Rady (UE) 2016 /1148 z dn. 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

sankcje na podmioty, które nie dostosują się do Dyrektywy NIS i nie wdrożą zabezpieczeń zapewniających spełnienie minimalnego poziomu bezpieczeństwa sieci i systemów.

Należy wspomnieć, że Dyrektywa NIS nakłada na kraje członkowskie obowiązek zachowania ciągłości funkcjonowania infrastruktury krytycznej, a co za tym idzie nakłada na podmioty odpowiedzialność za ciągłość działania i świadczenie tzw. usług krytycznych. W sektorze e-zdrowia są to usługi związane z zapewnieniem[21]:

a) ciągłości działania systemów informacji zdrowotnej przetwarzającej EDM,
b) dostępności repozytoriów danych czyli bazy danych w jednostkach, w którym informacja jest przechowywana lokalnie,
c) dostępności dla użytkowników systemów informatycznych realizowanej między innymi poprzez ciągłość pracy serwerów odpowiedzialnych za uwierzytelnianie tj. przeprowadzenie kontroli dostępu i uwierzytelniania użytkowników,
d) ciągłości działania informatycznych systemów laboratoryjnych - Laboratory Information System (LIS)
e) ciągłości działania informatycznych systemów radiologicznych - Radiology Information Systems (RIS)
f) dostępności elektronicznej dokumentacji medycznej zawartych w elektronicznych kartach zdrowia,
g) kluczowych usług niezbędnych do świadczenia opieki zdrowotnej.

W ramach krajowych przepisów obowiązujących w zakresie cyberbezpieczeństwa opracowywana jest obecnie przez Ministerstwo Cyfryzacji ustawa o krajowym systemie cyberbezpieczeństwa. Ustawa ma regulować krajowy system cyberbezpieczeństwa, którego zadaniem będzie zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług. Efektem tych działań będzie podniesienie odporności kluczowych usług świadczonych z wykorzystaniem technologii informatycznych na ataki pochodzące z cyberprzestrzeni. Tym samym projektowana regulacja przyczyni się do lepszego zapewnienia ciągłości działania tych usług, tak, aby zarówno obywatele jak i przedsiębiorstwa mieli do nich stały dostęp. W tym miejscu wskazać należy, że przez krajowy system cyberbezpieczeństwa będzie się rozumieć wszystkie nowe w obrocie prawnym podmioty, realizujące techniczne i organizacyjne zadania w systemie. System będzie obejmować operatorów usług kluczowych, dostawców usług cyfrowych, CSIRT Narodowy, narodowe centrum cyberbezpieczeństwa, CSIRT (ang. Computer Security Incident Response Team) sektorowe w tym tworzony przez CSIOZ CSIRT e-Zdrowie. Ustawa ma za zadanie utworzenie nowych rozwiązań systemowych i strukturalnych zajmujących się cyberbezpieczeństwem na poziomie technicznym, a więc narodowe centrum cyberbezpieczeństwa oraz CSIRT Narodowy. Narodowe centrum cyberbezpieczeństwa będzie prowadzić system teleinformatyczny, pozwalający na wymianę informacji

[21] Security and Resilience in eHealth Security Challenges and Risks European Union Agency For Network And Information Security 2016

i dzielenie się wiedzą co do zagrożeń, incydentów i podatności. Regulacja ta będzie również obejmować świadczeniodawców opieki zdrowotnej a więc podmioty wykonujące działalność leczniczą.

3. Odpowiedzialność wynikająca z przetwarzania dokumentacji medycznej w postaci elektronicznej

Każdy podmiot przetwarzający dane osobowe ponosi odpowiedzialność prawną za przestrzeganie aktualnie obowiązujących regulacji prawnych z tym związanych. Obecnie kluczowa w tym zakresie jest UODO, w pewnym zakresie zastosowanie mogą mieć również przepisy Kodeksu cywilnego oraz przepisy Kodeksu pracy.

Jednakże należy również pamiętać, że od 25 maja 2018 roku sytuacja ta ulegnie zmianie, gdyż od tego dnia zacznie obowiązywać 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).

3.1 Odpowiedzialność karna

Ustawodawca w rozdziale 8 UODO przewidział przepisy karne dotyczące nieprzestrzegania zasad przetwarzania danych osobowych.

Jednym z najważniejszych przepisów przedmiotowego rozdziału jest art. 51. Przedmiotem ochrony na gruncie przywołanego przepisu jest poufność danych osobowych w granicach wyznaczonych przez zasadę celowości i zasadę bezpieczeństwa danych. Zgodnie z tym przepisem:

„1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.”

Wskazać w tym miejscu należy równeież, że naruszenie omawianego przepisu może zostać popełnione tylko przez administrującego zbiorem danych osobowych lub osobę obowiązaną do ochrony danych osobowych. Zgodnie z tym przepisem „udostępnienie danych osobowych” polega na ich przekazaniu osobie nieuprawnionej. Natomiast „umożliwienie dostępu” może polegać m.in. na ujawnieniu kodu dostępu do zbioru danych osobowych. Oznacza to, że odpowiedzialność karna w przypadku

„umożliwienia dostępu" nie jest uzależniona od faktu czy osoba nieuprawniona zapoznała się faktycznie z danymi a jedynie od takiej możliwości[22].

Nie można wykluczyć, że w przypadku „wycieku" danych osobowych organ prowadzący postępowanie karne zastosuje kumulatywną kwalifikację czynu i obok omawianego art. 51 ust. 1 UODO wskaże również art. 266 § 1 kodeksu karnego. W świetle tego ostatniego przepisu, kto wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Ponadto administrator danych osobowych może odpowiadać za niezachowanie wymaganych środków zabezpieczeń. Zgodnie bowiem z art. 52 UODO - „kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku." Jak zostało wskazane w cytowanym powyżej przepisie znamieniem przestępstwa jest samo tylko niedopełnienie obowiązku ochrony danych osobowych, choćby dane te nie zostały zabrane lub uszkodzone. Jednak trzeba pamiętać, że w stanie faktycznym opisanym w przywołanym artykule dochodzi bowiem nie tylko do "umożliwienia dostępu", lecz także do umożliwienia zabrania tych danych przez osobę trzecią. Warto w tym miejscu również wskazać, że przestępstwo opisane w tymże artykule jest przestępstwem indywidualnym, które może być popełnione tylko przez administrującego danymi osobowymi. Inaczej niż w przepisach art. 51 oraz 53 UODO komentowany artykuł nie stanowi o "administrującym zbiorem danych", lecz o "administrującym danymi".

3.2 Odpowiedzialność cywilna

Ujawnienie danych osobowych osobom nieupoważnionym może również skutkować odpowiedzialnością cywilną. Możliwe są dwie podstawy takiej odpowiedzialności: z tytułu czynów niedozwolonych (deliktowa) oraz z tytułu naruszenia dóbr osobistych.

Ogólnym przepisem regulującym odpowiedzialność deliktową jest zawarty w księdze trzeciej Kodeksu cywilnego art. 415 odnoszący się do odpowiedzialności ex delicto. Przepis ten stanowi, że „kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia". Jeśli więc w wyniku niedopełnienia przez administratora danych osobowych lub osoby przez niego upoważnionej obowiązków zachowania danych w tajemnicy, osoba której te dane dotyczą poniosła jakąś szkodę na swoim majątku (np. ujawnione dane osobowe zostały wykorzystane do zaciągnięcia zobowiązania, zawarcia umowy) ma ta osoba prawo dochodzenia naprawienia wynikłej szkody.

Kolejnym z przepisów Kodeksu cywilnego umożliwiającym dochodzenie odpowiedzialności na gruncie prawa cywilnego może być przepis art. 23 wskazujący, że „dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek,

[22] http://www.ghmw.pl/odpowiedzialnosc-administratora-danych-osobowych-i-osob-przez-niego-upowaznionych-za-wyciek-powierzonych-danych-osobowych/

tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach". W związku z tym jeśli zostaną ujawnione nielegalnie dane osobowe np. dane dotyczące zdrowia co skutkować będzie, że dana osoba stanie się celem agentów ubezpieczeniowych osoba ta ma prawo ochrony swoich dóbr osobistych zgodnie z art. 24 przywołanego kodeksu. Przepis ten wskazuje, że „ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny".

3.3 Sankcje finansowe

Najważniejszym i jednocześnie najbardziej dotkliwym rodzajem sankcji przewidzianych w RODO są administracyjne kary pieniężne, o których mowa w art. 83 rozporządzenia.

Po pierwsze dlatego[23], że kary te będą nakładane przez organ kontrolny (w przypadku Polski zgodnie z projektem ustawy o ochronie danych organem kontrolnym będzie Prezes Urzędu Ochrony Danych Osobowych) bezpośrednio po stwierdzeniu naruszenia określonych wymogów RODO. Warto zauważyć, że na gruncie obecnie obowiązującej ustawy o ochronie danych osobowych Generalny Inspektor Ochrony Danych Osobowych nie może nakładać kar finansowych po stwierdzeniu naruszenia przepisów ustawy - w takim wypadku wydaje decyzję administracyjną, w której stwierdza naruszenie wymogów prawnych i wyznacza adresatowi decyzji termin na usunięcie uchybień. Dopiero w przypadku gdy te uchybienia nie zostaną usunięte w terminie wyznaczonym w decyzji, GIODO ma prawo nałożyć karę grzywny w celu "zmotywowania" danego podmiotu do realizacji jej postanowień.

Po wejściu w życie RODO będzie można nakładać kary bezpośrednio po stwierdzeniu naruszenia przepisów prawa i nie będzie musiał wyznaczać dodatkowego terminu na usunięcie uchybień by sankcja finansowa mogła być orzeczona (czyli w praktyce kara będzie orzekana już w samej treści decyzji administracyjnej jako sankcja za naruszenie określonych wymagań RODO).

Po drugie dlatego, że mogą sięgać ogromnych kwot (w skrajnych wypadkach nawet do wysokości 20 mln euro lub - gdy kara nakładana jest na przedsiębiorstwo - do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego).

Aktualnie wysokość kary grzywny jaką GIODO ma prawo nałożyć (w trybie, o którym mowa wyżej) każdorazowo może sięgać kwoty do 50 000 zł, a w przypadku nakładania grzywny wielokrotnie łącznie jej suma nie może przekroczyć 200 000 zł.

[23] https://www.odoekspert.pl/baza-wiedzy/odpowiedzialnosc-z-tytulu-naruszenia-przepisow-o-ochronie-danych-osobowych-dzis-i-jutro

Katalog naruszeń, które będą dawały podstawę do nałożenia administracyjnej kary pieniężnej w kwocie do 10 mln euro lub - gdy kara nakładana jest na przedsiębiorstwo - do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego zostały wskazane w art. 83 ust. 4 RODO.

Należą do nich między innymi:

a) niestosowanie mechanizmów uwzględniania ochrony danych w fazie projektowania (tzw. privacy by design) oraz domyślnej ochrony danych (tzw. privacy by default), o których mowa w art. 25 RODO,
b) naruszenie zasad współpracy pomiędzy współadministratorami danych, o których mowa w art. 26 RODO,
c) naruszenie obowiązków w zakresie powierzania do przetwarzania danych osobowych (w tym obowiązek korzystania przez administratorów danych wyłącznie z usług takich podmiotów przetwarzających, które spełniają wymagania RODO, czy też wymagania odnośnie formy i zakresu umowy, na podstawie której dochodzi do powierzenia przetwarzania danych),
d) naruszenie obowiązku prowadzenia rejestru czynności przetwarzania danych, o którym mowa w art. 30 RODO,
e) niestosowanie odpowiednich środków bezpieczeństwa zapewniających wymagany poziom ochrony danych osobowych (zgodnie z przeprowadzaną analizą ryzyka) - art. 32 RODO,
f) niezgłaszanie faktu naruszenia ochrony danych osobowych do organu kontrolnego oraz nieprzekazanie informacji o tym fakcie osobom, których te dane dotyczą (art. 33 i 34 RODO),
g) niestosowanie się do obowiązku przeprowadzania oceny skutków dla ochrony danych w sytuacjach gdy jest to wymagane (art. 35 RODO),
h) niewyznaczenie inspektora ochrony danych w przypadkach gdy to wyznaczenie jest obligatoryjne (art. 37 RODO) i wiele innych.

Katalog naruszeń, które będą dawały podstawę do nałożenia kary pieniężnej w kwocie do 20 mln euro lub - gdy kara nakładana jest na przedsiębiorstwo - do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego zostały wskazane w art. 83 ust. 5 RODO.

Należą do nich między innymi[24]:

a) niestosowanie się do podstawowych zasad przetwarzania danych, o których mowa w art. 5, 6, 7 oraz 9 RODO (chodzi między innymi o znane z polskiej ustawy o ochronie danych osobowych, aczkolwiek zmodyfikowane na gruncie RODO zasady legalności i celowości przetwarzania danych, wymagania prawne wobec zgody jako podstawy prawnej przetwarzania danych, czy też warunki przetwarzania danych sensytywnych),
b) naruszenie praw osób, których dane dotyczą, określonych w art. 12-22 RODO (m.in. wymagania wobec obowiązków informacyjnych jakie należy spełniać wobec tych osób, uprawnienia tych osób do dostępu, żądania sprostowania oraz w określonych w RODO

[24] Tamże

przypadkach żądania usunięcia ich danych, czy też prawo do przenoszenia danych pomiędzy różnymi administratorami danych),

c) naruszenie wymagań prawnych związanych z transferem danych osobowych do tzw. państw trzecich, o których mowa w art. 44-49 RODO.

W projekt ustawy o ochronie danych osobowych w art. 83 dot. administracyjnych kar pieniężnych ustawodawca zaproponował zapis dotyczący złagodzenia kar stosowanych wobec podmiotów publicznych

Ważne

Art. 83. 1. Na podmioty publiczne, o których mowa w art. 9 pkt 8 - 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870, z późn. zm.) Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 zł.

3.4 Prawo do odszkodowania

Niezależnie od administracyjnych kar pieniężnych, o których była mowa wyżej (i które będzie mógł nakładać organ kontrolny - w Polsce GIODO lub jego odpowiednik w innych krajach członkowskich UE), należy pamiętać, że zgodnie z treścią art. 82 ust. 2 RODO każdy administrator danych może ponosić bezpośrednią odpowiedzialność odszkodowawczą względem osób, których dane osobowe przetwarza. Odpowiedzialność odszkodowawczą będzie również ponosić podmiot, któremu powierzono do przetwarzania dane osobowe o ile nie dopełnił on przy przetwarzaniu danych obowiązków określonych dla tego typu podmiotów w RODO lub też gdy działał poza zgodnymi z prawem instrukcjami przekazywanymi przez administratora danych lub wbrew tym instrukcjom.

W przypadku gdy dojdzie do naruszeń wymagań rozporządzenia, każdej osobie, która poniosła szkodę majątkową lub niemajątkową z tego tytułu, przysługiwać będzie prawo żądania odszkodowania od podmiotu, który jest odpowiedzialny za ich powstanie. W przypadku gdy w tym samym procesie przetwarzania danych uczestniczyć będzie więcej niż jeden podmiot i wszystkie one będą odpowiedzialne za powstanie szkody związanej z naruszeniem wymagań RODO, podmioty te będą ponosiły odpowiedzialność solidarną za całą powstałą szkodę (a nie tylko do wysokości spowodowanej szkody przez każdy podmiot indywidualnie). Dzięki temu wystarczającym będzie np. skierowanie roszczenia tylko do jednego, wybranego podmiotu, który jest odpowiedzialny za naruszenia, a same roszczenie będzie mogło dotyczyć całej wyrządzonej szkody (a nie tylko "części" szkody za którą ten podmiot jest faktycznie odpowiedzialny)[25].

Bardzo ważne jest również to, że prawo do żądania odszkodowania ma charakter niezależny od innych możliwych sankcji przewidzianych w RODO. W praktyce więc prawdopodobnie często będzie miała

[25] Tamże

miejsce sytuacja, w której wobec podmiotu ,który naruszył postanowienia rozporządzenia Generalny Inspektor Ochrony Danych Osobowych nałoży administracyjną karę pieniężną, a poza tym roszczenia o odszkodowanie skierują wobec niego osoby, których dane były przetwarzane niezgodnie z wymaganiami RODO.

Prawa do odszkodowania z tytułu powstania szkody wynikającej z przetwarzania danych osobowych niezgodnie z postanowieniami rozporządzenia będzie można dochodzić na drodze postępowania sądowego.

3.5 Sankcje administracyjne

Ogólne rozporządzenie o ochronie danych przewiduje także możliwość korzystania przez organy kontrolne z tzw. uprawnień naprawczych, które stanowią rodzaj sankcji administracyjnych. Zgodnie z treścią art. 58 ust. 2 RODO każdemu organowi kontrolnemu przysługiwać będą między innymi następujące uprawnienia[26]:

a) wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów rozporządzenia poprzez planowane operacje przetwarzania,
b) udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów rozporządzenia przez realizowane operacje przetwarzania,
c) nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO,
d) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania danych do wymagań rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu w jakim należy się dostosować,
e) nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony jej danych osobowych,
f) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania danych,
g) nakazanie zawieszenia przepływu danych do odbiorcy zlokalizowanego w tzw. państwie trzecim lub do organizacji międzynarodowej.

Prezes Urzędu Ochrony Danych Osobowych korzystając z uprawnień naprawczych będzie mógł jednocześnie nałożyć na dany podmiot administracyjną karę pieniężną lub też poprzestać na zastosowaniu tylko jednego z tych środków (czyli albo uprawnienia naprawczego albo administracyjnej kary pieniężnej), przy czym decyzja w tym zakresie będzie należała do organu kontrolnego.

3.6 Pozostałe sankcje

[26] Tamże

Art. 84 RODO stanowi, że poszczególne państwa członkowskie UE mają wprowadzić również inne sankcje za naruszenia postanowień rozporządzenia. Tak więc należy założyć, że katalog tych środków zostanie jeszcze poszerzony.

Odnosząc się do aktualnie obowiązującej ustawy o ochronie danych osobowych warto zauważyć, że w Rozdziale 8 przewiduje ona odpowiedzialność karną. Aktualnie obowiązujące w Polsce przepisy prawa pracy pozwalają również pracodawcom stosować sankcje dyscyplinarne wobec pracowników, którzy nie przestrzegają zasad ochrony danych osobowych na swoich stanowiskach pracy i tym samym naruszają swoje obowiązki pracownicze.

Ogólne rozporządzenie o ochronie danych nie przewiduje wprost sankcji karnych czy też dyscyplinarnych, ale zachęca do ich wprowadzania. O możliwości wprowadzania sankcji karnych w ustawodawstwach państw członkowskich stanowi na przykład punkt 149 preambuły rozporządzenia (stanowi on między innymi że "Państwa członkowskie powinny mieć możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie niniejszego rozporządzenia, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach (...)"). Również biorąc pod uwagę treść art. 84 RODO należy przyjąć, że sankcje karne lub dyscyplinarne mogą być utrzymane przez poszczególne państwa w swoich ustawodawstwach.

Część IV. Zalecenia i rekomendacje dotyczące bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej

Prowadzenie dokumentacji medycznej w postaci elektronicznej umożliwia podmiotom udzielającym świadczeń zdrowotnych szybkie wprowadzanie i wyszukiwanie danych.

Zgodnie z DokMedR dokumentacja może być prowadzona w postaci elektronicznej, pod warunkiem prowadzenia jej w systemie teleinformatycznym zapewniającym:

- zabezpieczenie dokumentacji przed uszkodzeniem lub utratą;
- integralność treści dokumentacji i metadanych polegającą na zabezpieczeniu przed wprowadzaniem zmian, z wyjątkiem zmian wprowadzanych w ramach ustalonych i udokumentowanych procedur;
- stały dostęp do dokumentacji dla osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych;
- identyfikacja osoby dokonującej wpisu oraz osoby udzielającej świadczeń zdrowotnych i dokumentowanie dokonywanych przez te osoby zmian w dokumentacji i metadanych;
- przyporządkowanie cech informacyjnych dla odpowiednich rodzajów dokumentacji, zgodnie z § 10 ust. 1 pkt 3 DokMedR;
- udostępnienie, w tym przez eksport w postaci elektronicznej dokumentacji albo części dokumentacji będącej formą dokumentacji określonej w rozporządzeniu, w formacie, w którym jest ona przetwarzana (XML albo PDF);
- eksport całości danych w formacie określonym w przepisach wydanych na podstawie art. 13 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia;
- funkcjonalność wydruku dokumentacji.

Jednocześnie wskazać należy, że w przypadku, gdy do dokumentacji prowadzonej w postaci elektronicznej ma być dołączona dokumentacja utworzona w innej postaci, w tym zdjęcia radiologiczne lub dokumentacja utworzona w postaci papierowej, osoba upoważniona przez podmiot wykonuje odwzorowanie cyfrowe tej *dokumentacji* i umieszcza je w systemie informatycznym w sposób zapewniający czytelność, dostęp i spójność *dokumentacji*. W przypadku wykonania odwzorowania cyfrowego dokumentacja jest zwracana pacjentowi albo niszczona w sposób uniemożliwiający identyfikację pacjenta. Utrwalenie dokumentacji prowadzonej w postaci elektronicznej polega na zastosowaniu odpowiednich do ilości danych i zastosowanej technologii rozwiązań technicznych zapewniających przechowywanie, używalność i wiarygodność dokumentacji znajdującej się w systemie informatycznym co najmniej do upływu okresu przechowywania dokumentacji (§80- 82 DokMedR).

Dokumentacja medyczna jest udostępniana:

- do wglądu, w tym także do baz danych w zakresie ochrony zdrowia, w miejscu udzielania świadczeń zdrowotnych, z wyłączeniem medycznych czynności ratunkowych, albo w siedzibie

podmiotu udzielającego świadczeń zdrowotnych, z zapewnieniem pacjentowi lub innym uprawnionym organom lub podmiotom możliwości sporządzenia notatek lub zdjęć;

- przez sporządzenie jej wyciągu, odpisu, kopii lub wydruku;
- za pośrednictwem środków komunikacji elektronicznej;
- na informatycznym nośniku danych.

Dokumentację w postaci elektronicznej udostępnia się z zachowaniem jej integralności oraz ochrony danych osobowych. W przypadku gdy dokumentacja prowadzona w postaci elektronicznej jest udostępniana w postaci papierowych wydruków, osoba upoważniona przez podmiot potwierdza ich zgodność z dokumentacją w postaci elektronicznej i opatruje swoim oznaczeniem, zawierającym imię, nazwisko, stanowisko i podpis. Dokumentacja wydrukowana powinna umożliwiać identyfikację osoby udzielającej świadczeń zdrowotnych (§83 DokMedR).

Dokumentacja prowadzona w postaci elektronicznej jest właściwe zabezpieczona, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:

- jest zapewniona jej dostępność wyłącznie dla osób uprawnionych,
- jest chroniona przed przypadkowym lub nieuprawnionym zniszczeniem,
- wprowadzono metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

Zabezpieczenie dokumentacji w postaci elektronicznej wymaga w szczególności:

- systematycznego dokonywania analizy zagrożeń,
- opracowania i stosowania procedur zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu oraz przechowywania,
- stosowania środków bezpieczeństwa adekwatnych do zagrożeń,
- bieżącego kontrolowania funkcjonowania wszystkich organizacyjnych i technicznoinformatycznych sposobów zabezpieczania, a także okresowego dokonywania oceny skuteczności tych sposobów
- przygotowania i realizacji planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na nowe informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.

W celu zapewnienia bezpieczeństwa dokumentacji medycznej rekomendowane jest wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji. Na wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w organizacji mają wpływ wymagania bezpieczeństwa, procesy funkcjonujące oraz jej wielkość i struktura. Prawidłowo opracowany, wdrożony i ciągle doskonalony Systemu Zarządzania Bezpieczeństwem Informacji zapewnia zachowanie poufności, integralności i dostępności informacjom zawartym w dokumentacji medycznej w wyniku stosowania zarządzania ryzykiem. Jednocześnie w przypadku przeniesienia dokumentacji do innego systemu teleinformatycznego, do przeniesionej dokumentacji przyporządkowuje się datę przeniesienia oraz informację, z jakiego systemu została przeniesiona.

Dokumentację prowadzoną w postaci elektronicznej sporządza się z uwzględnieniem postanowień Polskich Norm, których przedmiotem są zasady gromadzenia i wymiany informacji w ochronie zdrowia,

przenoszących normy europejskie lub normy innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszące te normy.
W przypadku braku Polskich Norm przenoszących normy europejskie lub normy innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszące te normy uwzględnia się:

- normy międzynarodowe;
- Polskie Normy;
- europejskie normy tymczasowe.

1. Obowiązek zabezpieczenia danych medycznych

Obowiązek zabezpieczenia danych medycznych nakłada na usługodawcę UODO oraz DokPrzetwR. W niniejszym rozdziale uwzględniono również zalecenia rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016 r. poz. 113) oraz normy PN-ISO/IEC 27001 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji, PN-EN ISO 27799 Informatyka w ochronie zdrowia – Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002, normy PN-EN 13606-4:2009 Informatyka w ochronie zdrowia - Przesyłanie elektronicznej dokumentacji zdrowotnej - Część 4: Bezpieczeństwo danych, .

Należy podkreślić, że odpowiedzialność za zapewnienie wymaganego poziomu bezpieczeństwa przetwarzanych danych, w szczególności danych medycznych, określonego w aktach prawnych i normach ponosi usługodawca. W przypadku gdy zdecyduje się on na wybór rozwiązania, w którym część lub całość usług dostarcza podmiot zewnętrzny musi zawrzeć z nim umowę powierzenia przetwarzania danych osobowych. Przedmiotem powierzenia przetwarzania danych osobowych mogą być wszelkie operacje dokonywane na tych danych. W zakres pojęcia przetwarzania danych wchodzi także samo przechowywanie danych np. w ramach hostingu, archiwizacji ale także ich usuwania. Umowa powierzenia danych osobowych powinna określać m.in. cel i zakres przetwarzania danych, sposób wykonania umowy, odpowiedzialność wykonawcy, czas trwania umowy. Poprzez określenie celu przetwarzania danych osobowych należy rozumieć wskazanie potrzeby dla której dochodzi do powierzenia, może nią być utrzymywanie systemu przetwarzającego dane na serwerze zewnętrznym, przechowywania, usuwania danych osobowych zawartych na nośnikach danych. Natomiast zakres przetwarzania danych osobowych oznacza wskazanie w umowie konkretnych operacji przetwarzania danych jakie będą wykonywane przez podmiot, któremu administrator danych zleca. Zakresu przetwarzania danych nie powinno się utożsamiać z zakresem (kategoriami) danych osobowych, których przetwarzanie zostało powierzone. Wymienianie w umowie kategorii danych osobowych nie jest błędem ale nie zastępuje określenia zakresu powierzenia przetwarzania danych. Umowa z dostawcą usług powinna również zawierać klauzulę audytu umożliwiającą sprawdzenie dostawcy pod względem wymagań bezpieczeństwa. Kierownictwo organizacji na drodze regulacji wewnętrznych powinno również zobowiązać pracowników do przestrzegania określonych zasad w zakresie zapewnienia bezpieczeństwa danych medycznych oraz określić konsekwencje nieprzestrzegania tych zasad. Należy również stale dbać o podnoszenie świadomości kadry na wszystkich szczeblach organizacji w zakresie stosowania zasad Polityki Bezpieczeństwa. Umowa, zgodnie z dobrymi praktykami, powinna zawierać również zobowiązania podmiotu, któremu

przetwarzanie danych powierzono, do przekazywania administratorowi danych informacji dotyczących ewentualnych kontroli GIODO przeprowadzanych w tym podmiocie.

Ogólnie przez pojęcie zapewnienia ochrony przetwarzanym danym zawartym w dokumentacji medycznej należy rozumieć działanie mające na celu zabezpieczenie przed czymś szkodliwym, niekorzystnym, niebezpiecznym. W odniesieniu do dokumentacji medycznej zawierającej dane osobowe wrażliwe będą to działania mające na celu zapewnienie, aby były one pozyskiwane i przetwarzane zgodnie z przepisami prawa. Oznacza to między innymi, że powinny być one wykorzystywane tylko w określonym celu, zabezpieczone przed nieuprawnionymi zmianami, ujawnieniem nieupoważnionym osobom, zniszczeniem, utratą lub uszkodzeniem.

Czynności podejmowane w ramach tych działań oraz zastosowane środki techniczne i organizacyjne będą zależne między innymi od środowiska i technologii w jakim dokumentacja medyczna jest przetwarzana.

Pojęcie bezpiecznego przetwarzania elektronicznej dokumentacji medycznej należy w tym przypadku utożsamiać z pojęciem „bezpieczeństwa informacji", stosowanym w zakresie bezpieczeństwa teleinformatycznego. Według normy PN-ISO/IEC 27001:2014 przez bezpieczeństwo informacji należy rozumieć zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności i polegają odpowiednio na:

a) Poufności – zapewnieniu, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
b) Integralności – zapewnieniu, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
c) Dostępności – zapewnieniu bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
d) Rozliczalności – zapewnieniu, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
e) Autentyczności – zapewnieniu, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
f) Niezaprzeczalności – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
g) Niezawodności – zapewnieniu spójności oraz zamierzonych zachowań i skutków. Należy zwrócić uwagę, że zapewnienie a następnie wykazanie określonych właściwości wymaga często zastosowania określonych środków i jednoczesnego spełnienia wielu warunków.

Zapewnienie np. niezaprzeczalności podpisu elektronicznego (wykazanie, że dany dokument elektroniczny podpisała określona osoba) wymaga udowodnienia, że dany dokument nie został zmieniony (integralność), a złożony podpis należy do danej osoby (uwierzytelnienie). Gdy do przetwarzania danych osobowych wykorzystuje się systemy informatyczne, zadania dotyczące zapewnienia określonych właściwości przenoszone są na odpowiednie wymagania dotyczące właściwości tych systemów. Dodatkowy problem, jaki wówczas powstaje, polega na zapewnieniu skuteczności i ciągłości zachowywania przez systemy informatyczne wymaganych właściwości. Właściwości te mogą być utracone na skutek błędów popełnionych przez administratora systemu lub celowych działań osób nieupoważnionych do ingerowania w dany system informatyczny.

Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, ochronę przetwarzanych danych, należy zapewnić również ochronę systemu informatycznego, którego użyto do ich przetwarzania.

Zaleca się aby organizacja wyznaczyła osoby pełniące określone role, w szczególności osoby pełniące role Administratora Danych Osobowych oraz Administratora Bezpieczeństwa Informacji lub inne osoby, które będą odpowiedzialne za zapewnienie bezpieczeństwa danych w organizacji a także aby przydzielono im stosowne uprawnienia. Zgodnie z § 6 ust. 1[lxxviii] DokPrzetwR podmioty przetwarzające dane medyczne muszą zapewnić poziom bezpieczeństwa systemu informatycznego na poziomie co najmniej podwyższonym lub wysokim.

Poziom podwyższony stosuje się wówczas, gdy przetwarzane są dane, o których mowa w art. 27[lxxix] UODO oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Poziom wysoki natomiast stosuje się w przypadku, gdy co najmniej jedno urządzenie służące do przetwarzania danych osobowych jest połączone z siecią publiczną.

Administrator danych osobowych w myśl UODO ma obowiązek zapewnienia bezpieczeństwa przetwarzanych danych, tj. zapewnienia środków technicznych i organizacyjnych zapewniających ochronę danych osobowych.

Jednocześnie mając na uwadze zapisy art. 25 ust 1[lxxx] oraz art. 32 ust. 1[lxxxi] RODO w zakresie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych i bezpieczeństwa przetwarzania, placówka medyczna prowadząca dokumentację w postaci elektronicznej powinna zorganizować sposób gromadzenia informacji w taki sposób, aby nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji pod warunkiem, że informacje te są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, których celem jest zapewnienie spełnienia wymogów prawa w zakresie ochrony danych osobowych. Aby móc wykazać przestrzeganie prawa w tym zakresie, administrator danych 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 albo na szyfrowaniu tych danych lub 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 czy wybieraniu dostawców usług nieposiadających możliwości wglądu do przetwarzanych danych.

W trakcie opracowywania, projektowania, wybierania i użytkowania aplikacji, usług i produktów, które przetwarzają dane osobowe w ramach przetwarzania dokumentacji medycznej, należy wymagać od wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, 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 obowiązkach ochrony danych. Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy bezwzględnie brać pod uwagę w przetargach publicznych.

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

1.1 Pseudonimizacja i szyfrowanie

Zgodnie z definicją zawartą w RODO „pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

RODO jako odpowiednie zabezpieczenie obok pseudonimizacji wymienia szyfrowanie danych. Szyfrowanie to proces przekształcenia danych na niezrozumiały ciąg znaków w celu jego utajnienia. W zależności od tego czy do procesu deszyfrowania wykorzystywany jest ten sam klucz, który brał udział w procesie szyfrowania czy inny wyróżnić należy system kryptograficzny z kluczem tajnym (szyfrowanie symetryczne) oraz system kryptograficzny z kluczem publicznym (szyfrowanie niesymetryczne).

Pseudonimizacja danych osobowych może ograniczyć ryzyko dla osób, których dane dotyczą, oraz pomóc administratorom i podmiotom przetwarzającym wywiązać się z obowiązku ochrony danych. Tym samym bezpośrednie wprowadzenie pseudonimizacji nie służy wykluczeniu innych środków ochrony danych.

Pseudonimizacja nie jest jednoznaczna z anonimizacją ponieważ anonimizacja jest co do zasady procesem nieodwracalnym.

Podczas wyboru techniki pseudonimizacji, mając na uwadze aktualny stan technologii, należy uwzględnić trzy czynniki ryzyka:

1. wyodrębnienie, które pozwala na wydzielenie zapisów identyfikujących określoną osobę fizyczną w zbiorze;
2. możliwość tworzenia powiązań np. na podstawie analizy korelacji danych;
3. wnioskowanie ze znacznym prawdopodobieństwem wartości danego atrybutu na podstawie innych atrybutów zbioru.

Szczególnym ryzykiem jest uznawanie danych opatrzonych pseudonimem za równoważne ze zanonimizowanymi danymi. Nie można zrównać danych pseudonimicznych ze zanonimizowanymi

informacjami, ponieważ te pierwsze nadal umożliwiają wyodrębnienie konkretnej osoby fizycznej, której dane dotyczą. Istnieje prawdopodobieństwo, że w przypadku pseudonimowości możliwa będzie identyfikacja i dlatego technika ta jest objęta zakresem systemu prawnego dotyczącego ochrony danych. Jest to szczególnie istotne w kontekście badań naukowych, statystycznych lub historycznych.

Zarówno Dyrektywa 95/46/WE, jak i RODO nie wskazują, jakie techniki należy stosować do pseudonimizacji danych, stąd możliwe jest posiłkowanie się opinią 05/2014 w sprawie technik anonimizacji przedstawiającą techniki anonimizacji oparte na: randomizacji i uogólnieniu, opracowaną przez Grupę Roboczą Art. 29 w oparciu o analizę powyższych ryzyk. Opinia obejmuje także pseudonimizację oraz techniki prywatności różnicowej, l-dywersyfikacji, t-bliskości.

Grupa robocza szczegółowo omówiła pojęcie danych osobowych w opinii 4/2007 w sprawie danych osobowych, uwzględniając w szczególności elementy tworzące definicję przedstawioną w art. 2 lit. a) dyrektywy 95/46/WE, w tym część tej definicji, jaką jest sformułowanie „zidentyfikowanej lub możliwej do zidentyfikowania". W tym kontekście grupa robocza stwierdziła także, że „dane, którym nadano anonimowy charakter są danymi anonimowymi, które wcześniej dotyczyły osoby możliwej do zidentyfikowania, lecz której zidentyfikowanie nie jest już możliwe".

W związku z tym grupa robocza wyjaśniła, że w dyrektywie proponuje się przeprowadzenie testu *„sposobów, jakimi można się posłużyć"* jako kryterium, które należy zastosować w celu ocenienia, czy proces anonimizacji jest wystarczająco dokładny, tj. czy identyfikacja stała się praktycznie niemożliwa. Szczególny kontekst i okoliczności określonego przypadku mają bezpośredni wpływ na możliwość identyfikacji.

Pseudonimizacja polega na zastępowaniu jednego atrybutu (atrybutu który jest szczególnie wrażliwy w kontekście identyfikacji osoby której dane dotyczą) w zapisie innym atrybutem. W związku z tym nadal istnieje prawdopodobieństwo pośredniego zidentyfikowania osoby fizycznej; dlatego też stosowanie samej pseudonimizacji nie będzie skutkowało anonimowym zbiorem danych.

Ogranicza ona również możliwość tworzenia powiązań zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą; technika ta stanowi zatem użyteczny środek bezpieczeństwa, ale nie metodę anonimizacji.

Wynik pseudonimizacji może być niezależny od wartości początkowej (jak w przypadku numerów losowych generowanych przez administratora danych lub nazwiska wybranego przez osobę, której dane dotyczą) lub może opierać się na pierwotnych wartościach atrybutu lub zbioru atrybutów, np. funkcji skrótu lub układu szyfrowania.

Do najczęściej stosowanych technik pseudonimizacji należą:

a) szyfrowanie z kluczem tajnym: w tym przypadku posiadacz klucza może z łatwością ponownie zidentyfikować każdą osobę, której dane dotyczą. Następuje to poprzez odszyfrowanie zbioru danych, ponieważ dane osobowe nadal znajdują się w tym zbiorze danych, który jest zaszyfrowany. Zakładając, że zastosowano układ szyfrowania w oparciu o stan wiedzy naukowej i technicznej, możliwość odszyfrowania istnieje wyłącznie w przypadku, gdy znany jest klucz;

b) funkcja skrótu: oznacza funkcję, która z wkładu każdej wielkości (wkład może być jednym atrybutem lub zbiorem atrybutów) daje wynik stałej wielkości i której nie można odwrócić. Funkcja ta oznacza, że ryzyko odwrócenia, występujące przy szyfrowaniu, już nie istnieje. Jeżeli znany jest jednak zakres wartości wkładu przy funkcji skrótu, będzie on mógł zostać ponownie odtworzony za pomocą funkcji skrótu w celu uzyskania prawidłowej wartości dla konkretnego zapisu. Na przykład, jeżeli zbiór danych został poddany pseudonimizacji poprzez skrócenie numeru PESEL, można uzyskać ten numer, po prostu skracając wszystkie możliwe wartości wkładu i porównując wyniki z odpowiednimi wartościami ze zbioru danych. Funkcje skrótu są zwykle opracowane w taki sposób, aby można było prowadzić stosunkowo szybkie obliczenia i są przedmiotem ataków siłowych[27] . Można również utworzyć wstępnie obliczone tabele, aby umożliwić odwrócenie masowe dużego zbioru wartości skrótu;
c) stosowanie funkcji skrótu z losowym ciągiem znaków (w której do skracanego atrybutu dodaje się losowy ciąg znaków, ang. „salt") może ograniczyć prawdopodobieństwo uzyskania wartości wkładu, ale obliczanie wartości pierwotnego atrybutu ukrytej za wynikiem funkcji skrótu z losowym ciągiem może jednak nadal być wykonalne w ramach uzasadnionych środków[28];
d) funkcja skrótu z kluczem, w przypadku której klucz jest przechowywany: oznacza określoną funkcję skrótu, która wykorzystuje klucz tajny jako dodatkowy wkład (różni się ona od funkcji skrótu z losowym ciągiem znaków, ponieważ zazwyczaj ciąg losowy nie stanowi tajemnicy). Administrator danych może ponownie odtworzyć tę funkcję względem atrybutu, wykorzystując klucz tajny, ale znacznie trudniej jest odtworzyć ją atakującemu bez znajomości klucza. W takim przypadku liczba możliwości, które trzeba sprawdzić, jest na tyle duża, że ich sprawdzanie jest niepraktyczne;
e) szyfrowanie deterministyczne lub funkcja skrótu z kluczem, w przypadku której klucz jest usuwany: technika ta może być utożsamiona z wybieraniem losowego numeru jako pseudonimu dla każdego atrybutu w bazie danych, a następnie z usuwaniem tabeli korelacji. Rozwiązanie to pozwala ograniczyć ryzyko możliwości tworzenia powiązań między danymi osobowymi w zbiorze danych a danymi odnoszącymi się do tej samej osoby fizycznej w innym zbiorze danych, w którym używa się innego pseudonimu. Rozważając algorytm oparty na stanie wiedzy naukowej i technicznej, odszyfrowanie lub odtworzenie funkcji będzie dla atakującego trudne pod względem obliczeniowym, ponieważ wiązałoby się ono ze sprawdzaniem każdego możliwego klucza ze względu na fakt, iż klucz ten nie jest dostępny;
f) tokenizacja: technika ta jest zwykle stosowana w sektorze finansowym (chociaż nie tylko) w celu zastąpienia numerów identyfikacyjnych kart wartościami, które ograniczają użyteczność dla atakującego. Opiera się ona na omówionych wcześniej technikach i zwykle polega na stosowaniu mechanizmów szyfrowania jednokierunkowego lub na przypisaniu, za pomocą funkcji indeksu, sekwencji liczb lub losowo wygenerowanych liczb, które nie zostały w sposób matematyczny uzyskane z danych pierwotnych.

Jak już podkreślono, badania, narzędzia i moc obliczeniowa ulegają zmianom. Dlatego też przedstawienie wyczerpującego wyliczenia okoliczności, w których identyfikacja nie jest już możliwa,

[27] Ataki takie polegają na wypróbowaniu wszystkich możliwych kombinacji w celu utworzenia tabel korelacji.

[28] W szczególności, jeżeli znany jest rodzaj atrybutu (nazwisko, numer ubezpieczenia społecznego, data urodzenia itp.). W celu dodania wymogu obliczeniowego można opierać się na funkcji skrótu z wyprowadzaniem klucza, w której wyliczona wartość zostaje kilkukrotnie skrócona za pomocą krótkiego losowego ciągu znaków.

nie jest wykonalne ani użyteczne. Niektóre istotne czynniki zasługują jednak na uwzględnienie i omówienie.

Słabości pseudonimizacji

a) **Wyodrębnienie:** nadal możliwe jest wyodrębnienie zapisów poszczególnych osób, ponieważ dana osoba wciąż może zostać zidentyfikowana przez atrybut nietypowy, który wynika z funkcji pseudonimizacji (= atrybut pseudonimiczny).
b) **Możliwość tworzenia powiązań:** nadal łatwo będzie można tworzyć powiązania między zapisami, wykorzystując ten sam atrybut pseudonimiczny w celu odniesienia się do tej samej osoby fizycznej. Mimo, że do tej samej osoby fizycznej, której dane dotyczą, wykorzystuje się różne atrybuty pseudonimiczne, nadal będzie istniała możliwość tworzenia powiązań za pomocą innych atrybutów.
c) **Wnioskowanie:** ataki oparte na wnioskowaniu ukierunkowane na prawdziwą tożsamość osoby, której dane dotyczą, są możliwie w ramach zbioru danych lub między różnymi zbiorami danych, które wykorzystują te same atrybuty pseudonimiczne w odniesieniu do określonej osoby fizycznej, lub jeżeli pseudonimy nie wymagają wyjaśnienia i nie ukrywają w odpowiedni sposób prawdziwej tożsamości osoby, której dane dotyczą.

Powszechne błędy popełniane w zakresie stosowania technik pseudonimizacji.

Powszechnym błędem popełnianym w tym zakresie jest zakładanie przez administratorów danych, że dane opatrzone pseudonimem zostały zanonimizowane. W takim przypadku administratorzy danych często wychodzą z założenia, że usunięcie lub zastąpienie jednego atrybutu lub ich większej liczby wystarcza do zanonimizowania zbioru danych. Niestety wiele przykładów pokazało, że tak nie jest. Zwykła zmiana identyfikatora danych osobowych nie uniemożliwia zidentyfikowania osoby, której dane dotyczą, jeżeli w zbiorze danych pozostają quasi-identyfikatory lub jeżeli wartości innych atrybutów nadal umożliwiają zidentyfikowanie danej osoby fizycznej. W wielu przypadkach zidentyfikowanie konkretnej osoby fizycznej w zbiorze danych opatrzonych pseudonimem jest tak proste, jak w przypadku danych pierwotnych. Należy w takiej sytuacji podjąć dodatkowe działania w celu uznania zbioru danych za zanonimizowany, w tym usunąć i uogólnić atrybuty lub wykasować dane pierwotne albo przynajmniej sprawić, by były one w dużym stopniu zagregowane.

Powszechne błędy przy stosowaniu pseudonimizacji jako techniki ograniczania możliwości tworzenia powiązań:

a) **wykorzystywanie tego samego klucza w różnych bazach danych**: eliminowanie możliwości tworzenia powiązań różnych zbiorów danych polega w dużym stopniu na stosowaniu algorytmu kluczy oraz na fakcie, że jedna osoba będzie odpowiadała różnym atrybutom pseudonimicznym w różnych kontekstach. Dlatego, aby ograniczyć możliwości tworzenia powiązań, ważne jest unikanie wykorzystywania tego samego klucza w różnych bazach danych;
b) **wykorzystywanie różnych kluczy („kluczy zmienianych") w odniesieniu do różnych użytkowników**: może powstać pokusa wykorzystywania różnych kluczy w odniesieniu do różnych zbiorów użytkowników i zmiany klucza przy każdym użyciu (na przykład, użycie tego

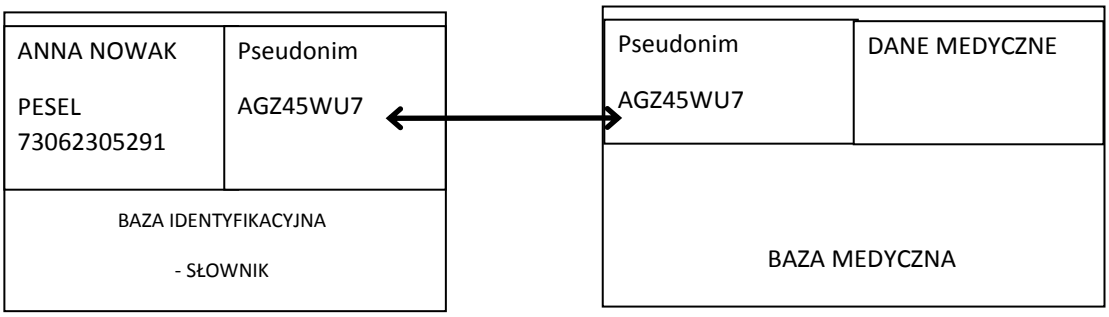
samego klucza do zarejestrowania 10 wpisów dotyczących tego samego użytkownika). Jeżeli jednak takie działanie nie jest odpowiednio zaprojektowane, może spowodować wystąpienie wzorców, co częściowo ograniczy zamierzone korzyści. Przykładowo zmienianie klucza w drodze stosowania szczególnych zasad w odniesieniu do konkretnych osób fizycznych ułatwiłoby możliwość tworzenia powiązań wpisów odpowiadających danym osobom. Również znikanie powtarzających się danych opatrzonych pseudonimem z bazy danych w czasie, gdy pojawiają się nowe, może sygnalizować, że oba zapisy odnoszą się do tej samej osoby fizycznej;

c) **zachowywanie klucza**: jeżeli klucz tajny jest przechowywany razem z danymi opatrzonymi pseudonimem, a dane zostają narażone na szwank, atakujący może być w stanie z łatwością powiązać dane pseudonimiczne z ich pierwotnymi atrybutami. Ta sama zasada ma zastosowanie, gdy klucz jest przechowywany oddzielnie od danych, ale nie w sposób bezpieczny.

W celu zwiększenia bezpieczeństwa danych osobowych, a także w celu zapewnienia zgodności systemów w których przetwarzane są dane medyczne, systemy te powinny korzystać możliwie z jak największej liczby metod służących pozbawieniu danych cech danych osobowych a więc deidentyfikacji, pseudonimizacji oraz zapewnienia niejednoznaczności. Dane zawierające dane osobowe powinny być przechowywane w modelu separacji danych, z zaleceniem stosowania modeli wielowarstwowych a uwzględniając wrażliwość danych medycznych stosowanie również wielowarstwowych modeli separacji z fizycznym (a nie elektronicznym) notariuszem.

Model pseudonimizacji z separacją danych bazuje przede wszystkim na podzieleniu danych na dwie części – odseparowanie danych wrażliwych (niosących w sobie informacje identyfikujące) od pozostałych danych. Oczywiście proces separacji od strony merytorycznej musi być przeprowadzony tak, aby odseparowane dane identyfikacyjne nie niosły ze sobą żadnej dodatkowej informacji, a jedynie informację identyfikacyjną. Powiązanie pomiędzy odseparowaną od danych częścią identyfikacyjną a samymi danymi realizowane jest za pośrednictwem pseudonimów. Mamy tu zatem do czynienia z kolejnymi etapami depersonalizacji (wydzielenia danych identyfikujących), pseudonimizacji (nadania pseudonimów powiązujących oba zestawy danych) oraz rozdzielenia logicznego obu zestawów danych.

Przykładem może być tu często stosowana procedura przechowywania obrazowych danych medycznych: zamiast przechowywania danych w całości w jednej bazie danych o wysokim stopniu zabezpieczeń, dane są separowane. Informacje czysto identyfikacyjne takie jak imię, nazwisko, adres, numer PESEL, itp. (zgodnie z listą pól identyfikujących) są wydzielane do odrębnej tabeli lub bazy danych i opatrywane pseudonimem. Odpowiadające im dane obrazowe opatrzone tym samym pseudonimem przechowywane są w drugiej tabeli lub bazie. Ogólną zasadę działania tego modelu w najprostszej postaci pokazuje poniższy rysunek.

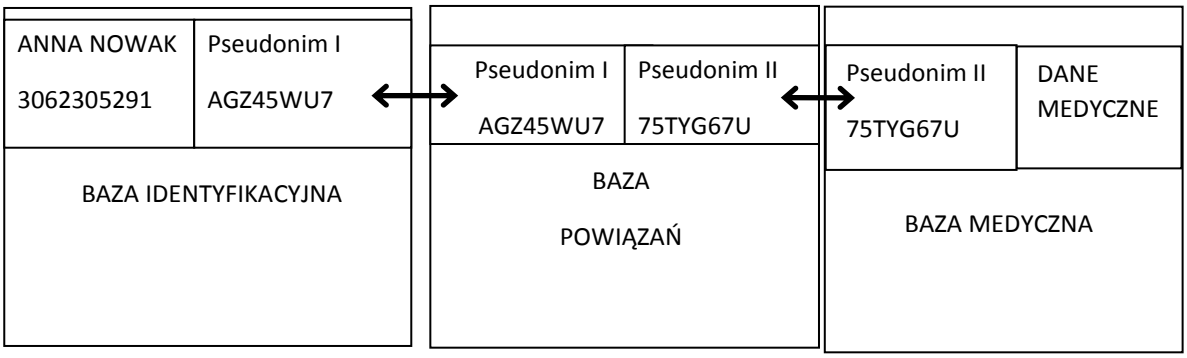


Rys. 2 - Model separacji

Oddzielenie danych wrażliwych od pozostałej części danych powoduje, że każdy z dwóch nowopowstałych zestawów danych nie niesie sam w sobie żadnej kluczowej, niebezpiecznej informacji. Baza identyfikacyjna zawiera same dane identyfikacyjne, bez danych medycznych – pomimo, że są to nadal dane osobowe, to nie zawierają żadnej dodatkowej informacji poza czystymi danymi identyfikującymi, a przede wszystkim nie zawierają wrażliwych informacji o stanie zdrowia pacjenta. Minusem jest jednak fakt, że jednoczesny, nieautoryzowany dostęp do obu baz powoduje od razu utratę poufności danych – w konsekwencji istnienia jawnej relacji.

Zwiększenie bezpieczeństwa może nastąpić również przez fizyczne rozdzielenia obu zestawów danych – tak aby każdy z nich był przechowywany w innej bazie, a nawet idąc krok dalej na innym serwerze, czy nawet w innej organizacji. W ten sposób bardzo maleje ryzyko jednoczesnego nieautoryzowanego dostępu do obu zestawów danych, a co za tym idzie znacząco wzrasta poziom bezpieczeństwa i poufności danych wrażliwych. Często również stosowanym rozwiązaniem jest przechowywanie bazy słownikowej w środowisku odciętym od sieci komputerowej, czasem nawet zamkniętej w sejfie, co zapewnia w jeszcze większym stopniu ochronę samych danych osobowych, a jednocześnie umożliwia pracę na pseudonimach.

Ponieważ jednak nadal istnieje ryzyko złamania dostępu do obu baz, lub utraty poufności np. przez dostęp administracyjny, poprzez bezpośrednią relację pseudonimów w obu bazach, wprowadza się rozwiązania o jeszcze wyższym stopniu zabezpieczeń – pseudonimy wielowarstwowe. W modelu wielowarstwowym, zarówno rekord w bazie identyfikującej, jak i rekord w bazie medycznej mają nadawany osobny pseudonim. Powiązanie pomiędzy odpowiadającymi sobie rekordami jest realizowane za pośrednictwem dodatkowej warstwy – bazy powiązań (linking database). Ta dodatkowa baza jest kluczem do odtworzenia powiązania pomiędzy pacjentem a jego danymi medycznymi i zawiera jedynie zestawienia obu pseudonimów z obu baz. Model ten przedstawiony jest na Rys. 2. W takim modelu newralgicznym elementem bezpieczeństwa całości jest bezpieczeństwo bazy powiązań. Nawet jednoczesny, nieautoryzowany dostęp do bazy identyfikacyjnej i medycznej nie umożliwia dokonania połączenia pomiędzy tymi dwoma zestawami danych, gdyż brakuje relacji. Dopiero wykorzystanie bazy powiązań pozwala na pełne odtworzenie relacji. Z drugiej strony dostęp jedynie do bazy powiązań, bez jednoczesnego dostępu do baz identyfikującej i medycznej również nie narusza poufności danych.



Rys. 3 - Model separacji wielowarstwowej.

Częstym rozwiązaniem praktycznym jest wprowadzenie niejako osobnej instancji w miejsce bazy powiązań – czy to organizacji, czy też osoby, gwarantującej zarówno nadawanie pseudonimów po każdej ze stron, jak i przechowywanie skojarzeń pseudonimów. Jednostka ta często nazywana jest też nadzorcą lub notariuszem i może być prowadzona zarówno w wersji elektronicznej (umożliwiającej systemowe wykorzystanie relacji), jak i w bardziej wrażliwych przypadkach w postaci „fizycznej", niedostępnej elektronicznie.

Należy pamiętać, że w przypadku przekazywania do przetwarzania danych w celach innych niż cel w którym dane zostały zebrane, dane muszą zostać zanonimizowane, czyli przygotowane w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować.

1.2 Bezpieczeństwo stosowania pseudonimizacji i szyfrowania

Wprowadzając zabezpieczenia związane z pseudonimizacją i szyfrowaniem danych, zaleca się opracować procedury stosowania zabezpieczeń kryptograficznych.

W związku z powyższym niezbędnym jest określenie:

a) wymaganego poziomu ochrony, opartego na szacowaniu ryzyka oraz biorącego pod uwagę typ, siłę i jakość wymaganych algorytmów kryptograficznych;

b) zasad korzystania z kryptografii do zabezpieczania informacji transportowanych w przenośnych lub na wymiennych nośnikach i urządzeniach albo przesyłanych za pośrednictwem linii komunikacyjnych;

c) sposobu zarządzania kluczami, w tym metody bezpiecznego udostępniania kluczy kryptograficznych, odzyskiwania zaszyfrowanych informacji w przypadku utraty oraz naruszenia bezpieczeństwa lub uszkodzenia kluczy bądź przejęcia urządzenia przenośnego. Dzięki technologii kryptograficznej umożliwiającej podział kluczy prywatnych użytkownika funkcjonują mechanizmy, które uniemożliwiają uzyskanie dostępu do danych przez osoby nieuprawnione nawet w przypadku gdy zostaną przejęte dane uwierzytelniające. Użytkujący urządzenie przenośne powinien jeśli to możliwe zastosować odpowiednie środki kryptograficzne wobec przechowywanych na nim danych osobowych i/lub danych medycznych. W szczególności musi wykorzystywać system informatyczny

umożliwiający szyfrowanie lokalne przy jednoczesnym zastosowaniu technologii podziału kluczy szyfrujących (gdzie jedna z cząstek klucza jest przechowywana poza urządzeniem). Alternatywą do powyższego jest wykorzystywanie systemu służącego do kryptograficznej ochrony danych bazującego na technologii chmury obliczeniowej i podziale oraz wymianie kluczy szyfrujących – wówczas dane przechowywane są w postaci zaszyfrowanej na serwerze, a nie na urządzeniu użytkownika.

d) ról i odpowiedzialności;

e) standardów, które mają zostać przyjęte do skutecznego wdrożenia;

f) wpływu korzystania z zaszyfrowanej informacji na zabezpieczenia, które opierają się na analizie treści (np. wykrywanie szkodliwego oprogramowania).

Zalecanym jest równocześnie, aby podjęcie decyzji w kwestii tego, czy użycie rozwiązania kryptograficznego jest właściwe, było częścią szerszego procesu szacowania ryzyka i wyboru zabezpieczeń. Szacowanie to może być podstawą stwierdzenia, czy zabezpieczenie kryptograficzne jest właściwe i jaki typ zabezpieczenia należy zastosować, do jakich celów i procesów związanych przetwarzaniem danych.

Procedury stosowania zabezpieczeń kryptograficznych są potrzebne, aby maksymalizować korzyści i minimalizować ryzyko związane z używaniem technik kryptograficznych oraz aby uniknąć nieodpowiedniego lub niepoprawnego użycia.

Jednocześnie należy pamiętać, że podczas opracowywania procedur, zaleca się ustanowić i wdrożyć zabezpieczenia w zakresie korzystania, ochrony i okresów ważności kluczy kryptograficznych. oraz trzeba uwzględnić wymagania dotyczące zarządzania kluczami kryptograficznymi w czasie całego ich cyklu życia obejmujące generowanie, przechowywanie, archiwizację, odzyskiwanie, dystrybucja, wycofywanie i niszczenie kluczy. Zaleca się również, aby wszystkie klucze były chronione przed modyfikacją, utratą lub zniszczeniem. Warto tym miejscu również pamiętać, że klucze tajne oraz prywatne wymagają ochrony przed nieuprawnionym ujawnieniem, a urządzenia używane do generowania, przechowywania i archiwizowania kluczy podlegały fizycznej ochronie.

Zaleca się wybieranie algorytmów szyfrowania, długości kluczy i praktyki stosowania zgodnie z najlepszymi praktykami. Właściwe zarządzanie kluczami wymaga bezpiecznych procesów generowania, przechowywania, archiwizacji, odzyskiwania, dystrybucji, wycofywania i niszczenia kluczy kryptograficznych.

System zarządzania kluczami opierać się musi na standardach, procedurach i metodach zabezpieczania w celu:

a) generowania kluczy dla różnych systemów kryptograficznych i różnych aplikacji;

b) generowania i otrzymywania certyfikatów klucza publicznego;

c) przekazywania kluczy do zamierzonych podmiotów, w tym określenie sposobu aktywowania kluczy po ich otrzymaniu;

d) przechowywania kluczy, w tym metody uzyskiwania dostępu do nich przez uprawnionych użytkowników;

e) zmiany lub aktualizacji kluczy, w tym zasady, według których jest zalecana wymiana kluczy oraz sposób, w jaki to robić;

f) postępowania z kluczami, których bezpieczeństwo zostało naruszone;

g) unieważniania kluczy, w tym metody wycofywania kluczy z użycia lub ich dezaktywacji, np. po naruszeniu bezpieczeństwa kluczy lub, gdy ich użytkownik opuści organizację (w takim wypadku zaleca się archiwizowanie kluczy);

h) odtwarzania kluczy, które zostały utracone lub uszkodzone;

i) kopiowania lub archiwizowania kluczy;

j) niszczenia kluczy;

k) rejestrowania i audytu czynności związanych z zarządzaniem kluczami.

W celu zmniejszenia prawdopodobieństwa niewłaściwego użycia, koniecznym jest zdefiniowanie dla kluczy dat aktywacji i dezaktywacji, tak aby klucze mogły być używane jedynie przez ograniczony czas określony we właściwej procedurze zarządzania kluczami.

Wymagane jest również, aby w porozumieniach i umowach dotyczących świadczenia usług zawieranych z zewnętrznymi dostawcami usług kryptograficznych, np. z ośrodkiem certyfikacji, uwzględniały one takie kwestie, jak odpowiedzialność cywilnoprawna.

1.3 Stosowanie podpisu elektronicznego, kwalifikowanego podpisu elektronicznego i podpisu potwierdzonego Profilem Zaufanym

W niniejszym rozdziale zostały opisane wymagania prawne wynikające z USIOZ regulującej kwestie związane z elektroniczną dokumentacją medyczną oraz z rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania. Przedstawiony opis zawiera odniesienia do definicji podpisu elektronicznego, kwalifikowanego podpisu elektronicznego, Profilu Zaufanego, sposobu ich pozyskiwania i używania. Określone zostały również wymagania co do zakresu funkcjonalnego systemów elektronicznej dokumentacji medycznej w obszarze podpisu elektronicznego oraz podpisu systemowego o którym mowa w ust. 1 pkt 3 lit. e. Podpis systemowy, może być złożony oraz weryfikowany przy wykorzystaniu wewnętrznych mechanizmów systemu teleinformatycznego, o którym mowa w § 80 wskazanego powyżej rozporządzenia.

Przyjęty przez ustawodawcę obowiązek podpisywania elektronicznej dokumentacji medycznej przy użyciu kwalifikowanego podpisu elektronicznego lub podpisu potwierdzonego Profilem Zaufanym ma na celu zapewnienie integralności, niezaprzeczalności i autoryzacji tejże dokumentacji. Podpis elektroniczny w tym również podpis systemowy należy stosować zawsze gdy jest tworzona dokumentacja medyczna w postaci elektronicznej lub gdy wprowadzane są do niej zmiany. Każdy

system wspomagający funkcjonowanie EDM musi być wyposażony w moduły odpowiedzialne za pełną obsługę podpisu elektronicznego.

Wskazać w tym miejscu należy, że w ustawie USIOZ wskazano, że poprzez EDM należy rozumieć dokumenty wytworzone w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym Profilem Zaufanym:

a) umożliwiające usługobiorcy uzyskanie od usługodawcy świadczenia opieki zdrowotnej określonego rodzaju, z wyłączeniem zleceń na wyroby medyczne,

b) określone w przepisach wydanych na podstawie art. 13a.

1.3.1. Definicje związane z podpisem elektronicznym

Infrastruktura klucza publicznego (ang. Public Key Infrastructure (PKI)) - Zbiór osób, polityk, procedur i systemów komputerowych niezbędnych do świadczenia usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego i prywatnego oraz certyfikatów elektronicznych. PKI jest szeroko pojętym krypto-systemem, w skład którego wchodzą urzędy certyfikacyjne (CA), urzędy rejestracyjne (RA), subskrybenci certyfikatów klucza publicznego (użytkownicy), oprogramowanie oraz sprzęt. Infrastruktura klucza publicznego tworzy hierarchiczną strukturę zaufania, której podstawowym dokumentem jest certyfikat klucza publicznego. Najpopularniejszym standardem certyfikatów PKI jest X.509 w wersji trzeciej.

Urząd certyfikacji, centrum certyfikacji – podmiot, który wystawia certyfikaty cyfrowe. Certyfikat potwierdza własność klucza publicznego poprzez wskazanie podmiotu certyfikatu. Pozwala to innym powołującym się stronom polegać na podpisach lub zapewnieniach złożonych przez klucz prywatny odpowiadającemu kluczowi publicznemu, który jest certyfikowany. W powyższym modelu relacji zaufania, CA jest zaufaną stroną trzecią, której zawierzają zarówno podmiot (właściciel) certyfikatu oraz strona polegająca. Urzędy certyfikacji są charakterystyczne dla wielu systemów infrastruktury klucza publicznego (PKI).

Podpis elektroniczny - oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis.

Certyfikat podpisu elektronicznego - oznacza poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby.

Kwalifikowany podpis elektroniczny - oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

Kwalifikowany certyfikat podpisu elektronicznego - oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

Dostawca usług zaufania- oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania.

Kwalifikowany dostawca usług zaufania- oznacza dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru.

1.3.2. Podpis elektroniczny i jego skutki prawne

Szczegółowe skutki prawne stosowania podpisu elektronicznego przedstawione zostały w art. 25 ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014. Najważniejsze z nich to:

1. Podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych.
2. Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu.
3. Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich.

Polskie prawodawstwo skutki prawne użycia podpisu elektronicznego reguluje np. w art. 78^1. ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2017 r. poz. 459, z późn. zm.):

1. w § 1. Do zachowania elektronicznej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym.
2. w § 2. Oświadczenie woli złożone w formie elektronicznej jest równoważne z oświadczeniem woli złożonym w formie pisemnej

1.3.3. Definicje związane z Profilem Zaufanym

Profil Zaufany – zestaw informacji identyfikujących i opisujących podmiot lub osobę będącą użytkownikiem, który został w wiarygodny sposób potwierdzony przez organ podmiotu określonego w ustawie o informatyzacji podmiotów realizujących zadania publiczne. Zawiera on zgodnie z § 8 ust. 1 rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r.
w sprawie profilu zaufanego elektronicznej platformy usług administracji publicznej (Dz. U. 1633):

1. Imię (imiona) użytkownika;
2. nazwisko użytkownika;
3. numer PESEL użytkownika;

4. identyfikator użytkownika;
5. identyfikator Profilu Zaufanego;
6. czas jego potwierdzenia;
7. termin ważności;
8. adres poczty elektronicznej użytkownika;
9. numer telefonu komórkowego;
10. wybrany przez użytkownika sposób autoryzacji.

Podpis potwierdzony Profilem Zaufanym – podpis złożony przez użytkownika konta, do którego zostały dołączone informacje identyfikujące zawarte w Profilu Zaufanym, a także:

a) jednoznacznie wskazujący Profil Zaufany osoby, która wykonała podpis,

b) zawierający czas wykonania podpisu,

c) jednoznacznie identyfikujący konto osoby, która wykonała podpis,

d) autoryzowany przez użytkownika konta,

e) opatrzony i chroniony pieczęcią elektroniczną wykorzystywaną w ePUAP w celu zapewnienia integralności i autentyczności wykonania operacji przez system.

1.3.4. Profil Zaufany i jego skutki prawne

Szczegółowe skutki prawne stosowania Profilu Zaufanego zawarte są w art. 20b ustawy z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne:

1. Podpis potwierdzony Profilem Zaufanym wywołuje skutki prawne, jeżeli został utworzony lub złożony w okresie ważności tego profilu.
2. Dane w postaci elektronicznej opatrzone podpisem potwierdzonym Profilem Zaufanym są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym, chyba że przepisy odrębne stanowią inaczej.
3. Nie można odmówić ważności i skuteczności podpisowi potwierdzonemu Profilem Zaufanym tylko na tej podstawie, że istnieje w postaci elektronicznej lub zmianie uległy dane inne niż służące do potwierdzenia profilu zaufanego.

2. Bezpieczeństwo fizyczne w obszarach przetwarzania danych osobowych w tym w szczególności danych medycznych

Na podstawie przeprowadzonej analizy ryzyka i planu postępowania z ryzykiem, których obowiązek przeprowadzenia wynika z art. 36 ust. 1[lxxxii] UODO oraz od 25 maja 2018 r. art. 32 RODO, każdy podmiot ma obowiązek wdrożenia odpowiednich środków bezpieczeństwa. W związku z tym w zakresie ochrony fizycznej należy rozważyć wyznaczenie obszarów bezpiecznych oraz podział na strefy w zależności od ich dostępności zarówno dla personelu, jak i pacjentów oraz przedstawicieli podmiotów współpracujących.

Podział na strefy umożliwia dobór stosowanych zabezpieczeń fizycznych:

1. Identyfikatory osobowe,
2. System kontroli dostępu,
3. Zarządzanie kluczami tradycyjnymi oraz elektronicznymi w postaci kart dostępu –wszystkie klucze powinny być przechowywane w zabezpieczonym miejscu, do którego dostęp mają wyłącznie osoby upoważnione,
4. System monitorowania wizyjnego,
5. Systemy przeciwwłamaniowe,
6. Zabezpieczenie okien i drzwi np. podwyższenie klasy drzwi (klasa C), folie zabezpieczające, folie lustrzane,
7. Służba ochrony całodobowa lub po godzinach pracy,
8. Systemy przeciwpożarowe lub gaśnice,
9. Klimatyzacja,
10. Czujniki temperatury i wilgotności.

Zgodnie z DokPrzetwR zabezpieczenia na poziomie wysokim w zakresie bezpieczeństwa fizycznego, a takim podlegają dane medyczne, powinny zapewniać co najmniej aby:

1. Obszar, w którym przetwarzane są dane osobowe, zabezpieczony był przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
2. Przebywanie osób nieuprawnionych w obszarze, w którym przetwarza się dane osobowe, było dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

Generalny Inspektor Ochrony Danych Osobowych określił przykładowe środki ochrony fizycznej w zakresie bezpieczeństwa danych osobowych:

1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.

3. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
4. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
5. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.
7. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
8. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.
9. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony.
10. Zbiór danych osobowych w postaci papierowej przechowywany jest w zamkniętej niemetalowej szafie.
11. Zbiór danych osobowych w postaci papierowej przechowywany jest w zamkniętej metalowej szafie.
12. Zbiór danych osobowych w postaci papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej.
13. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
14. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie.
15. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.
16. Zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.
17. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
18. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

Przykłady te nie wykluczają stosowania innych indywidualnie dobranych środków bezpieczeństwa, innych aktów prawnych np. ustawy o ochronie informacji niejawnych oraz standardów i norm.

W aspekty bezpieczeństwa fizycznego i środowiskowego RODO nie ingeruje, w związku z tym należy kierować się wskazaniami normy ISO 27002 oraz normy ISO 27799, które będą przydatne Administratorowi danych lub powołanemu IOD w sytuacji kiedy:

- dokonuje audytu i może porównać zaobserwowany stan zabezpieczeń fizycznych z dobrymi praktykami wskazanymi w normach;

- dokonuje oceny ryzyka naruszenia praw i wolności, niezależnie czy w ramach realizowanego obecnie sposobu doboru środków odpowiednich do zagrożeń i kategorii przetwarzanych danych czy już zgodnie z RODO;

- planując postępowanie z ryzykiem w zakresie zabezpieczeń fizycznych.

2.1 Obszary bezpieczeństwa

Fizyczna granica obszaru bezpiecznego

Norma ISO 27002 zawiera zalecenia, aby granice wyznaczonego obszaru bezpieczeństwa były solidne, wyposażone w bariery, których autoryzowane przekroczenie wymaga uwierzytelnienia (np. przy pomocy ewidencjonowanych i zaprogramowanych kart dostępu) oraz aby w przypadku nieautoryzowanego wejścia wywoływały alarm lub przynajmniej nie mogły zostać niezauważone. Poszczególne strefy obszarów przetwarzania mogą być rozdzielane kolejnymi, odrębnymi barierami, których przekroczenie wymaga odrębnych uprawnień, gdy upoważnienia do przetwarzania danych są zróżnicowane.

Uzupełniająca norma ISO 27799 zaleca określenie granic bezpieczeństwa i wykorzystanie ich w celu zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji. Organizacje zajmujące się przetwarzaniem informacji o zdrowiu powinny określić obszary bezpieczeństwa w taki sposób, aby chronić obszary, w których zbiera się oraz przetwarza dane o stanie zdrowia ale także obszary wymagające ochrony prywatności pacjenta. Te bezpieczne obszary powinny być chronione odpowiednimi elementami kontroli dostępu, w sposób zapewniający dostęp tylko dla uprawnionych pracowników.

1. Fizyczne zabezpieczenie wejść

   a. rejestrowania daty i godziny wejścia i wyjścia gości, nadzorowania ich pobytu w obszarach bezpiecznych, chyba że ich dostęp został wcześniej zaakceptowany; przyznawania dostępu gościom wyłącznie w określonych i zaaprobowanych celach oraz zapoznania ich z instrukcjami dotyczącymi wymagań bezpieczeństwa obszaru oraz z procedurami awaryjnymi. Tożsamość gości powinna być uwierzytelniona odpowiednimi środkami (np. okazanie dokumentu tożsamości lub podpis). Czynności te powinny być utrwalone w tzw. księdze gości;
   b. ograniczenia dostępu do obszarów, gdzie są przetwarzane lub przechowywane informacje poufne tylko dla uprawnionego personelu, poprzez wdrożenie właściwych zabezpieczeń dostępu, np. dwuskładnikowego mechanizmu uwierzytelnienia, takiego jak karta dostępu z kodem PIN;
   c. zobowiązania wszystkich pracowników, kontrahentów i podmiotów zewnętrznych do noszenia w widocznym miejscu jakiejś formy identyfikatora, a w przypadku zauważenia osoby bez takiego identyfikatora i bez towarzyszącej osoby nadzorującej, do zgłoszenia tego faktu ochronie;
   d. prowadzenia, bezpiecznego przechowywania i nadzorowania, książki rejestracji gości lub elektronicznego śladu, w których na potrzeby audytu umieszczane są zapisy wszystkich wejść;

e. przyznawania personelowi pomocniczemu reprezentującemu podmiot zewnętrzny ograniczonego dostępu do obszarów bezpiecznych lub środków przetwarzania informacji poufnych tylko wtedy, gdy jest to wymagane; autoryzowanie i monitorowanie takiego dostępu;
f. regularnego przeglądania praw dostępu do obszarów bezpiecznych i, jeśli zachodzi taka potrzeba, uaktualniania ich lub odbierania.

Oprócz wskazówek podanych przez ISO 27002, organizacje zajmujące się przetwarzaniem informacji o zdrowiu powinny podejmować rozsądne kroki, aby zapewnić, że pacjent jest tak blisko urządzeń IT (serwerów, urządzeń pamięci masowej, terminali i wyświetlaczy) jak wymaga tego proces leczenia.

2. Zabezpieczenie biur, pomieszczeń i obiektów.

W tym zakresie najważniejszymi zaleceniami są umieszczania kluczowych zasobów tak aby ograniczyć do nich dostęp osób nieupoważnionych, dlatego też kluczowym jest aby urządzenia sieciowe były zainstalowane w serwerowni, a drukarki nie stały w strefach publicznie dostępnych, o ile nie zastosowano innego sposobu zabezpieczenia np. wydruk poufny, wydruk podążający.

3. Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi.

Zaleca się korzystanie ze specjalistycznego doradztwa w kwestii tego, jak uniknąć zniszczeń powstałych na skutek pożaru, zalania, trzęsienia ziemi, wybuchu, niepokojów społecznych i innych form katastrof, naturalnych lub spowodowanych przez człowieka.

4. Praca w obszarach przetwarzania informacji.

Zaleca się uświadomienie personelu w zakresie istnienia obszaru bezpiecznego oraz prowadzonych w nim działań zgodnie z zasadą wiedzy koniecznej.

W obszarach przetwarzania danych medycznych prace wykonywane przez osoby nieupoważnione powinny być prowadzone wyłącznie pod nadzorem z powodów bezpieczeństwa, jak i z uwagi na uniemożliwienie złośliwych działań.

Zaleca się zamykanie i okresowe sprawdzania obszarów bezpiecznych, w których nie przebywają ludzie.

Nie wolno dopuszczać do korzystania z urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających, np. kamer w urządzeniach przenośnych, w obszarach przetwarzania danych chyba że osoba ma odpowiednie upoważnienie.

5. Obszar dostawy i załadunku

Obszar dostawy i załadunku należy traktować jako śluzę, przez którą zewnętrzni dostawcy nie powinni przedostawać się do obszarów przetwarzania danych a dostarczane przesyłki powinny być kontrolowane w odpowiedni sposób.

Zaleca się rejestrowanie dostarczanych materiałów zgodnie z procedurami zarządzania aktywami po dostarczeniu na miejsce, sprawdzanie przychodzących materiałów pod kątem tego, czy nie zostały

naruszone w czasie transportu. Jeśli taka ingerencja została wykryta, zaleca się natychmiastowe powiadomienie pracowników działu bezpieczeństwa.

Oprócz wskazówek przyjętych przez ISO / IEC 27002, norma ISO/IEC 27799 rekomenduje, aby pamiętać, że świadczenie opieki zdrowotnej obejmuje odrębne okoliczności, w których fizycznie dopuszczone są osoby fizyczne (obszary opieki pacjenta, pacjent i osoby towarzyszące) w obszarach o dużej wrażliwości (p. testy laboratoryjne, w których proces diagnostyczny może wymuszać gromadzenie informacji od osób objętych opieką w tym samym obszarze, w którym aktualnie przetwarzane są dane z poprzednich pacjentów, miejsca leczenia w nagłych przypadkach, w których osoby towarzyszące, krewni mogą mieć przypadkowy dostęp do znacznych ilości wrażliwych, ustnych i wizualnych informacje na temat innych podmiotów opieki, stacji roboczych i urządzeń diagnostycznych przy łóżku pacjenta/ stacje pielęgniarskich zlokalizowanych w pobliżu pomieszczeń pacjentów). Te obszary fizyczne w opiece zdrowotnej, zbierające informacje o zdrowiu poprzez wywiady i informacje z systemów, w których dane są wyświetlane na ekranie, powinny podlegać dodatkowej kontroli. W celu zapewnienia ochrony prywatności osób będących przedmiotem opieki zdrowotnej.

2.2 Zabezpieczenie sprzętu

Celem zabezpieczenia sprzętu jest zapobieżenie utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.

Zaleca się umieszczenie i ochronę sprzętu w taki sposób, aby zminimalizować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu.
W celu ochrony sprzętu zaleca się rozważenie ulokowania sprzętu w taki sposób, aby zminimalizować niepotrzebny dostęp do obszarów pracy, takiego ulokowania środków przetwarzania wrażliwych informacji, aby podczas ich użycia minimalizować ryzyko podglądu przez nieuprawnione osoby, urządzenia przechowujące informacje powinny być zabezpieczone w sposób uniemożliwiający nieuprawniony dostęp, wprowadzenie zabezpieczeń minimalizujących ryzyko związane z potencjalnymi zagrożeniami fizycznymi i środowiskowymi, np. kradzieżą, pożarem, środkami wybuchowymi, dymem, zalaniem (lub awarią zaopatrzenia w wodę), kurzem, wibracjami, środkami chemicznymi, interferencjami linii zasilających, linii komunikacyjnych, promieniowaniem elektromagnetycznym i wandalizmem. Zaleca się wprowadzenie procedur związanych ze spożywaniem posiłków, napojów oraz paleniem tytoniu w bliskim sąsiedztwie środków przetwarzania informacji.
Strefy przetwarzania danych, przede wszystkim serwerownie powinny być monitorowe pod względem takich warunków środowiska, jak temperatura i wilgotność, w celu wykrycia ich niekorzystny wpływ na działanie środków przetwarzania informacji.
Zaleca się wyposażenie wszystkich budynków w instalację odgromową oraz stosowania filtrów odgromowych na liniach zasilających i komunikacyjnych.
Oprócz wskazówek podanych przez ISO / IEC 27002, norma ISO /ICE 27799 wskazuje, iż organizacje zajmujące się przetwarzaniem informacji o zdrowiu powinny umieszczać stacje robocze umożliwiające dostęp do osobistych informacji o zdrowiu w sposób zapobiegający przypadkowemu przeglądowi lub dostępowi przez osoby opiekujące się pacjentem (osoby towarzyszące, krewni) oraz osoby postronne.

Urządzenia medyczne, które rejestrują lub raportują dane o stanie zdrowia, mogą wymagać szczególnych względów bezpieczeństwa w odniesieniu do środowiska, w którym działają w tym np. pola elektromagnetycznego.

2.3 Systemy wspomagające

Systemy wspomagające to przede wszystkim zasilanie, łączność i inne media (kanalizacja, wentylacja, gaz, klimatyzacja itp.), które są niezbędne do nieprzerwanej działalności podmiotu przetwarzającego dane.
Zaleca się aby systemy te był regularnie monitorowane i oceniane pod kątem ich zdolności do zaspokojenia wzrastających potrzeb biznesowych i interakcji z innymi systemami wspomagającymi, były regularnie sprawdzane i testowane, aby zapewnić ich prawidłowe funkcjonowanie a w razie potrzeby, generowały alarmy w celu wykrycia usterek. Należy zadbać aby w razie potrzeby, miały wiele kanałów zasilania biegnących różnymi trasami fizycznymi.
Zaleca się zapewnienie oświetlenia awaryjnego i awaryjnej łączności. Zaleca się umieszczenie awaryjnych wyłączników oraz zaworów wyłączających zasilanie, wodę, gaz oraz inne systemy wspomagające przy wyjściach awaryjnych lub pomieszczeniach ze sprzętem.

2.4 Bezpieczeństwo okablowania

Zaleca się, aby okablowanie zasilające i telekomunikacyjne, przenoszące dane lub wspomagające usługi informacyjne, było chronione przed przechwyceniem, zakłóceniem lub uszkodzeniem.
W kwestii bezpieczeństwa okablowania zaleca się rozważenie wdrożenia tam, gdzie jest to możliwe, prowadzenie linii zasilających i telekomunikacyjnych do środków przetwarzania informacji pod ziemią lub zabezpieczenie ich w inny stosowny sposób, oddzielenie kabli zasilających od okablowania komunikacyjnego w celu uniknięcia interferencji.
Zaleca się aby dla systemów wrażliwych lub krytycznych rozważyć dodatkowe zabezpieczenia obejmujące instalację zbrojonych rur kablowych i zamykanych pomieszczeń lub szafek w punktach kontrolnych i zakończeń, korzystanie z ekranów elektromagnetycznych do ochrony kabli, prowadzanie przeglądów technicznych oraz fizycznych inspekcji pod kątem nieautoryzowanych urządzeń podłączonych do kabli oraz kontrolowanie dostępu do paneli połączeniowych i pomieszczeń z okablowaniem.

Poza wskazaniami podanymi przez ISO / IEC 27002, norma ISO / IEC 27799 wskazuje, iż w podmiotach ochrony zdrowia powinno się poważnie rozważyć ochronę sieci i innego okablowania w obszarach o wysokich emisjach z urządzeń medycznych.

2.5 Konserwacja sprzętu

W celu zapewnienia ciągłej dostępności i integralności sprzętu zaleca się jego prawidłową konserwację zgodnie z zaleceniami dostawcy, w zakresie częstotliwości i zakresu, naprawianie lub serwisowanie sprzętu tylko przez autoryzowany personel, rejestrowanie wszystkich podejrzewanych lub rzeczywistych awarii oraz prewencyjnych i korygujących czynności konserwacyjnych.

Zaleca się wdrożenie odpowiednich zabezpieczeń na czas czynności konserwacyjnych, z uwzględnieniem działań przeprowadzanych przez personel na miejscu lub poza siedzibą organizacji; jeśli zachodzi taka potrzeba, usuwanie poufnych informacji ze sprzętu lub nadanie personelowi utrzymującemu odpowiednich uprawnień, zapewnienie zgodności z wszystkimi wymaganiami dotyczącymi konserwacji, nakładanymi przez polisy ubezpieczeniowej. Należy pamiętać o skontrolowaniu urządzenia przed jego ponownym uruchomieniem, po przeprowadzeniu jego konserwacji, w celu zapewnienia, że sprzęt nie został zmanipulowany i nie realizuje szkodliwych funkcji.

2.6 Wynoszenie aktywów

Zaleca się, aby sprzęt, informacje lub oprogramowanie nie były wynoszone poza siedzibę organizacji bez uzyskania wcześniejszego zezwolenia.
Zaleca się rozważenie zabezpieczeń w postaci procedur oraz na przykład wskazanie pracowników i użytkowników reprezentujących podmioty zewnętrzne, którzy mają prawo wynoszenia aktywów, jeśli to potrzebne i właściwe, rejestrowanie kiedy aktywa są wynoszone i kiedy są zwracane, dokumentowanie tożsamości, stanowiska i przynależności każdego, kto obsługuje lub wykorzystuje aktywa oraz zwrotu tej dokumentacji z urządzeniem, informacją lub oprogramowaniem.
Wyrywkowe kontrole, podejmowane w celu wykrycia aktywów wynoszonych bez zezwolenia, mogą być też wykorzystywane do wykrycia nieautoryzowanych urządzeń rejestrujących, broni itp. oraz chronić przed ich wniesieniem lub wyniesieniem z siedziby. Zaleca się przeprowadzanie takich kontroli zgodnie z odpowiednimi przepisami prawa i regulacjami. Jeśli kontrole są przeprowadzane, to należy o nich poinformować, a ich wykonanie autoryzować zgodnie z wymaganiami prawa i regulacjami.
Oprócz wdrożenia kontroli podanej przez ISO / IEC 27002, norma ISO / IEC 27799 zaleca aby podmioty zewnętrzne dostarczające lub wykorzystujące sprzęt, dane lub oprogramowanie wspierające aplikację służącą ochronie zdrowia zawierającą informacje o zdrowiu osobistym, nie miały możliwości usuwanie takich urządzeń, danych lub oprogramowania lub wynoszenia poza organizację bez zgody tej organizacji.

2.7 Bezpieczeństwo sprzętu i aktywów poza siedzibą

Zaleca się zabezpieczenie aktywów wynoszonych poza siedzibę organizacji przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą.
Zaleca się, aby korzystanie ze środków przechowywania i przetwarzania informacji poza siedzibą organizacji było autoryzowane przez kierownictwo. Ma to zastosowanie zarówno do urządzeń, jakimi dysponuje organizacja, jak i prywatnych, używanych w imieniu organizacji.
W kwestii ochrony sprzętu znajdującego się poza siedzibą, zaleca się nie pozostawiać w miejscach publicznych bez nadzoru urządzeń lub nośników wynoszonych poza siedzibę, przestrzegać instrukcji producenta dotyczących ochrony sprzętu, np. ochrony przed wystawieniem na działanie silnego pola elektromagnetycznego. Zaleca się stosować odpowiednie zabezpieczenia określone w czasie procesu szacowania ryzyka, niezbędne podczas pracy poza siedzibą, np. w domu, pracując zdalnie, w tymczasowych lokalizacjach, takie jak zamykane szafki, polityka czystego biurka, zabezpieczenia dostępu do komputerów oraz bezpieczne połączenie z biurem (patrz ISO/IEC 27033). Ważnym elementem jest dokumentacja , w której odnotowywany jest łańcuch posiadaczy

odpowiedzialnych za sprzęt, w tym co najmniej ich dane oraz nazwy organizacji, jeśli sprzęt znajdujący się poza siedzibą jest przenoszony pomiędzy różnymi osobami lub podmiotami zewnętrznymi.
Zaleca się, aby wybierając właściwe zabezpieczenia uwzględnić fakt, że ryzyka np. uszkodzeń, kradzieży lub podsłuchu, mogą znacząco różnić się w zależności od miejsca. W przypadku wystąpienia ryzyka kradzieży, utraty sprzętu na którym przechowywane są istotne dane np. dane wrażliwe, informacje na sprzęcie powinny być przechowywane w formie zaszyfrowanej. Nie niweluje to ryzyka kradzieży ale uniemożliwia dostęp do informacji osobom nieuprawnionym w przypadku utraty kontroli nad urządzeniem.
Oprócz wdrożenia kontroli podanej przez ISO / IEC 27002, norma ISO / ICE 27799 zaleca aby organizacje zajmujące się przetwarzaniem informacji o zdrowiu osobiście musi zapewnić, że wszelkie użycie urządzeń medycznych, które rejestrują dane lub raportuje, poza jej siedzibą, odbywa się zgodnie z upoważnieniem. Powinno to obejmować sprzęt wykorzystywany przez pracowników zdalnych, nawet tam, gdzie użytkowanie poza siedzibą odbywa się w sposób ciągły (tzn. gdy stanowi podstawowe narzędzie dla pracownika, np. dla personelu karetek pogotowia, terapeutów itp.).

2.8 Bezpiecznie zbywanie lub przekazywanie do ponownego użycia

Przed zbyciem lub przekazaniem sprzętu do ponownego użycia zaleca się sprawdzanie wszystkich jego składników zawierających nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.
Zaleca się aby nośniki danych były usuwane z urządzeń zbywanych lub przekazywanych do ponownego użycia.
Zaleca się fizyczne niszczenie nośników informacji zawierających informacje wrażliwe lub chronione prawem autorskim; zamiast standardowego kasowania lub formatowania zaleca się zniszczenie, skasowanie lub nadpisanie informacji za pomocą technik uniemożliwiających ich odtworzenie.
Uszkodzone urządzenia zawierające nośniki informacji mogą wymagać szacowania ryzyka określającego, czy należy je fizycznie zniszczyć, wysłać do naprawy, czy też wyrzucić. Nieostrożne zbycie lub przekazanie urządzenia do ponownego użycia może bowiem spowodować nieautoryzowane ujawnienie informacji.
Gdy sprzęt jest usuwany lub przeznaczony do ponownego użycia, to w celu zmniejszenia ryzyka ujawnienia poufnych informacji można zastosować dodatkowo, zamiast bezpiecznego wyczyszczenia dysku, jego zaszyfrowanie, pod warunkiem że proces szyfrowania jest wystarczająco silny i obejmuje cały dysk (w tym przestrzeń nieużywaną, pliki wymiany itp.), klucze szyfrowania są wystarczająco długie, aby zapewnić odporność na ataki wyczerpujące, same klucze szyfrowania są poufne (np. nigdy nie są przechowywane na tym samym dysku).
Techniki bezpiecznego nadpisywania nośników informacji różnią się w zależności od technologii tych nośników. Zaleca się przeglądanie narzędzi nadpisywania w celu upewnienia się, że mogą mieć one zastosowanie do danej technologii nośnika informacji.
Oprócz zaleceń wskazanych w normie ISO / IEC 27002, norma ISO / ICE 27799 organizacja przetwarzająca dane o stanie zdrowia musi bezpiecznie usunąć albo zniszczyć wszystkie nośniki zawierające informacje o stanie zdrowia pacjenta.

2.9 Pozostawianie sprzętu bez opieki

Zaleca się, aby użytkownicy zapewniali odpowiednią ochronę sprzętu pozostawianego bez opieki.
Zaleca się, aby wszyscy użytkownicy byli świadomi wymagań i procedur ochrony wyposażenia pozostawianego bez opieki, jak również odpowiedzialności związanej z wdrożeniem tej ochrony. Zaleca się użytkownikom, aby:
a) zamykali aktywne sesje po zakończeniu pracy, chyba że są one zabezpieczane przez odpowiedni mechanizm blokujący, np. wygaszacz ekranu chroniony hasłem;
b) wyrejestrowywali się z aplikacji lub usług sieciowych, kiedy nie są już więcej potrzebne;
c) zabezpieczali nieużywane w danym momencie komputery osobiste lub urządzenia mobilne przed nieupoważnionym dostępem poprzez blokadę klawiatury lub w inny równoważny sposób, np. dostęp do komputera po podaniu hasła.

2.10 Polityka czystego biurka i czystego ekranu

Zaleca się wprowadzenie polityki czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz polityki czystego ekranu dla środków przetwarzania informacji.
Zaleca się, aby polityka czystego biurka i czystego ekranu brała pod uwagę klasyfikację informacji, wymagania prawne i umowne oraz odpowiednie rodzaje ryzyka i uwarunkowania kulturowe organizacji.
Zaleca się rozważenie wprowadzenia następujących rozwiązań organizacyjnych:
a) przechowywania pod zamknięciem (najlepszym rozwiązaniem jest sejf, szafa lub inna forma zabezpieczenia) nieużywanych, wrażliwych lub krytycznych informacji biznesowych, np. umieszczonych na nośnikach elektronicznych lub w postaci dokumentów papierowych, szczególnie jeśli pomieszczenie biurowe jest opuszczane;
b) zamykania sesji lub blokowanie komputerów i terminali pozostawionych bez opieki za pomocą mechanizmu blokowania ekranu i klawiatury zabezpieczanego hasłem, tokenem lub z użyciem innego podobnego mechanizmu uwierzytelnienia użytkownika; ochrony komputerów i terminali mechanicznym zamkiem, hasłem lub za pomocą innego zabezpieczenia jeśli nie są używane;
c) wprowadzenia zakazu korzystania z kopiarek lub innych technik kopiowania (np. skanerów, aparatów cyfrowych) bez autoryzacji;
d) niezwłoczne usuwanie z drukarek wydruków zawierających wrażliwe lub klasyfikowane informacje.
Polityka czystego biurka i czystego ekranu ogranicza ryzyko nieautoryzowanego dostępu, utraty lub uszkodzenia informacji w czasie normalnych godzin pracy i poza normalnymi godzinami pracy. Ponadto, sejfy lub inne formy bezpiecznych urządzeń przechowujących mogą chronić przechowywane informacje przed takimi katastrofami, jak: pożar, trzęsienie ziemi, zalanie czy eksplozja.
Należy rozważyć korzystanie z drukarek chronionych cyfrowym kodem osobistym (PIN), aby tylko właściciele wydruku mogli otrzymać swoją kopię i tylko wtedy, gdy stoją obok drukarki.

3. Bezpieczeństwo systemów informatycznych i dokumentacji medycznej

W sytuacji przetwarzania danych medycznych, o których mowa w art. 27 UODO, stosuje się poziom podwyższony a jeżeli system ten połączony jest z siecią publiczną poziom wysoki. Za system połączony

z siecią publiczną uważa się taki w którym chociaż jeden z użytkowników łączy się z systemem ze stanowiska połączonego z siecią.

Zgodnie DokPrzetwR zabezpieczenia na poziomie wysokim w zakresie bezpieczeństwa systemów informatycznych przetwarzających dane medyczne powinny zapewniać co najmniej aby:

1. W systemie informatycznym służącym do przetwarzania danych osobowych zastosowane były mechanizmy kontroli dostępu do tych danych, a w przypadku, kiedy dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, zapewnione było, aby:
    a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
    b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
2. Jednocześnie zapewnić należy aby identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie mógł być przydzielony innej osobie.
3. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
4. System informatyczny służący do przetwarzania danych osobowych zabezpieczony był, w szczególności przed:
    a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
    b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
5. Dane osobowe przetwarzane w systemie informatycznym zabezpieczone muszą być przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
6. Kopie zapasowe muszą być:
    a) przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
    b) przechowywane jeżeli to możliwe w formie zaszyfrowanej;
    c) usuwane niezwłocznie po ustaniu ich użyteczności.
7. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
    a) likwidacji — muszą zostać pozbawione wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — muszą zostać pozbawione wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
    c) naprawy — muszą zostać pozbawione wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
8. Systemy informatyczne służące do przetwarzania danych osobowych muszą być chronione przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. W przypadku zastosowania logicznych zabezpieczeń, o których mowa powyżej, muszą one obejmować:

a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

9. Administrator danych musi stosować środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej, które uniemożliwiają uzyskanie dostępu do danych przez osoby nieuprawnione nawet w przypadku gdy zostaną one przez nie przejęte.
10. Osoba użytkująca komputer przenośny zawierający dane osobowe musi zachowywać szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym dane są przetwarzane, w tym muszą zostać zastosowane środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
11. Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1[lxxxiii] UODO, przekazywane poza obszar, w którym dane są przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność tych danych m.in. poprzez przechowywanie ich na tych urządzeniach i nośnikach w formie zaszyfrowanej.

Standardem jest stosowanie wygaszaczy ekranowych ze zwłoką czasową oraz koniecznością wprowadzenia hasła przy wznowieniu pracy w systemie informatycznym.

Dobrą praktyka jest okresowy przegląd uprawnień i identyfikatorów użytkowników, który może być realizowany przez porównanie anulowanych upoważnień z kontami aktywnymi w systemie informatycznym. Przegląd taki należy wykonywać regularnie, a w przypadku podmiotów publicznych co najmniej raz w roku. Przegląd taki może być częścią sprawdzenia prowadzonego przez administratora bezpieczeństwa informacji.

Zasady bezpieczeństwa dla poszczególnych modeli zostały opisane w następujących załącznikach:

Załącznik 1 – Model klasyczny,

Załącznik 2 – Kolokacja,

Załącznik 3 – Chmura obliczeniowa IaaS oraz hosting,

Załącznik 4 – Chmura obliczeniowa PaaS,

Załącznik 5 – Chmura obliczeniowa SaaS.

Spełnienie opisanych w Załącznikach wymagań zapewnia zgodność z ww. normami. Warto zaznaczyć, że ich wdrożenie jest pomocne dla zapewnienia zgodności z przepisami prawa. Każdy usługodawca ma możliwość wyboru dowolnego rozwiązania opisanego w rozdziale 3 niniejszego dokumentu, jednak po przeprowadzeniu analizy uwzględniającej również prawne uwarunkowania (w tym ograniczenia) w przypadku jego wdrożenia.

Należy podkreślić, iż ostateczny wybór powinien w pierwszej kolejności być uzależniony od wyników przeprowadzonej analizy ryzyka, potrzeb biznesowych, możliwości zarówno finansowych, lokalizacyjnych i kadrowych danej jednostki. Usługodawca powinien jednak przede wszystkim dokonać analizy prawnej wykorzystania danego modelu z uwzględnieniem wszystkich indywidualnych okoliczności wdrożenia.

Decydując się na wybór określonego modelu przetwarzania danych usługodawca określa podział odpowiedzialności pomiędzy siebie a podmiot zewnętrzny nad wykorzystywanymi zasobami IT, w zakresie zapewnienia bezpieczeństwa.

4. Bezpieczeństwo cyberprzestrzeni

Istnieje wiele standardów i dobrych praktyk wypracowanych przez różnego rodzaju instytucje. Do najpopularniejszych należy Standard Reagowania na Incydenty Bezpieczeństwa Komputerowego (ang. Computer Security Incidents Handling Guide), czyli tzw. norma NIST 800-61 opracowana przez Narodowy Instytut Standardów i Technologii przy amerykańskim Departamencie Handlu. Jest to standard uniwersalny, który może być stosowany w sektorze ochrony zdrowia. W największym uproszczeniu, zgodnie z normą NIST 800-61, kroki do zapewnienia cyberbezpieczeństwa są następujące.

1. **Przygotowanie.** Kluczowy i czasochłonny krok wymagający zidentyfikowania potencjalnych źródeł incydentów komputerowych, zbadania słabych stron zabezpieczenia komputerów i ich sieci, wyznaczenia osób odpowiedzialnych za zapewnienie cyberbezpieczeństwa (np. wyznaczenia wewnętrznego lub zewnętrznego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)) wraz z określeniem zakresów odpowiedzialności poszczególnych osób oraz opracowaniem procedur postępowania i zasad raportowania w przypadku zaistnienia incydentu.
2. **Identyfikacja incydentu.** Jeżeli monitoring działania systemu wykaże odstępstwa od normy, istnieje ryzyko, że nastąpił cyberatak. Wyzwaniem jest nie tylko jego zidentyfikowanie, ale też określenie rodzaju i skali spowodowanego zagrożenia dla bezpieczeństwa danych.
3. **Odpowiedź na incydent**. Musi być nie tylko adekwatna do zagrożenia, ale też szybka, aby ograniczyć do minimum skalę szkód. Na przykład odcięcie od systemu komputera zainfekowanego nielegalnym oprogramowaniem pozwoli ograniczyć wyciek informacji do danych przechowywanych na tym komputerze, a nie we wszystkich komputerach w sieci.
4. **Eliminacja przyczyny.** Po jej ustaleniu niezbędne jest wyłączenie czynnika ryzyka na przyszłość, np. zaktualizowanie oprogramowania antywirusowego, przeszkolenie pracowników w zakresie bezpiecznego korzystania z poczty elektronicznej.
5. **Powrót do normalnej działalności**. W zależności od skali cyberataku powrót do normalnej działalności może przebiegać w kilku etapach, np. powrót do świadczenia doraźnej pomocy medycznej, potem powrót do wykonywania niezbędnych zabiegów ratujących życie, a dopiero później wznowienie zabiegów planowych. Od strony informatycznej będzie to wymagało odzyskania dostępu do dokumentacji medycznej oraz wykonania niezbędnych kopii zapasowych.
6. **Usprawnienie systemu.** To krok ostatni, o którym nie można zapominać, ponieważ każdy cyberincydent w długofalowej perspektywie powinien przyczyniać się do wzmocnienia systemu ochrony danych pacjentów. Po wykonaniu wcześniejszych kroków rolą osoby odpowiedzialnej za cyberbezpieczeństwo jest przygotowanie raportu podsumowującego dla dyrekcji szpitala,

zawierającego wnioski i rekomendacje dotyczące zapobiegania analogicznym incydentom w przyszłości. Oznacza to zwykle, że praca nad sześcioma w/w punktami zaczyna się od nowa.

5. Praktyczny plan działania dla wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w podmiocie przetwarzającym dokumentację medyczną

Osoby odpowiedzialne za wdrażanie SZBI w podmiotach przetwarzających dokumentację medyczną przekonują się, że większość swoich celów kontrolnych będzie miało zastosowanie w niemal każdej sytuacji. Jednak użytkownicy standardu ISO/IEC 27001 w opiece zdrowotnej muszą uwzględniać, że mogą być potrzebne dodatkowe cele kontrolne. Są to często miejsca w których przecinają się procesy realizowane przez specjalistyczne urządzenia, takie jak skanery, urządzenia infuzyjne, etc., nawet jeśli kontrola bezpieczeństwa odnosi się jedynie do utrzymania integralności danych w konkretnym urządzeniu. Należy mieć również na uwadze różne ramy prawne, które mogą zmieniać zakres zgodności SZBI z normą ISO /IEC 27001. Norma ISO / IEC 27001 wprowadza pojęcie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz opisuje potrzebę stosowania szczegółowych rozwiązań w zakresie zapewnienia bezpieczeństwa informacjom opierając się przy tym o zasadę „privacy by design", oznaczającą wprowadzenie niezbędnych zabezpieczeń przetwarzanej dokumentacji medycznej. Aby sprostać celowi zapewnienia bezpieczeństwa jako istotne na wstępie przeprowadzenie identyfikacji i klasyfikacji informacji przetwarzanej w systemach informatycznych ochrony zdrowia, oraz na tej podstawie dokonanie oceny ryzyka. Zasady bezpieczeństwa informacji wynikające z najlepszych praktyk dowodzą, że w toku zgodność z normą ISO / IEC 27001[29] najlepiej jest zapewnić je poprzez wdrożenie systemu zarządzania zintegrowanego z ładem informacyjnym w danej organizacji.

5.1 Etapy wdrożenia SZBI

Wdrożenie SZBI obejmuje kilka etapów:

1. **tworzenie planu postępowania z ryzykiem**: jeżeli zagrożenia zostały zidentyfikowane na podstawie analizy ryzyka, to ryzyko powinno być zbadane i albo zaakceptowane przez kierownictwo wyższego szczebla lub zredukowane jeżeli ryzyko to jest uważane za niedopuszczalne. Plan redukcji ryzyka precyzuje działania, które muszą być przeprowadzone, aby zmniejszyć poziom niedopuszczalnego ryzyka. Obejmuje on plan wdrażania kontroli bezpieczeństwa wybranych zagrożeń, mających na celu ich redukcję lub akceptację. SZBI jest odpowiedzialny za zapewnienie, że plan ten jest przeprowadzany. Najlepiej, plan redukcji ryzyka będą obejmować harmonogramy, priorytety i szczegółowe

[29] PN-EN ISO 27001:2014 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania

plany pracy, a także przydzielenie odpowiedzialności za prowadzenia kontroli bezpieczeństwa. W opiece zdrowotnej, zatwierdzanie takich planów jest kluczowym etapem związanym z postępowaniem z ryzykiem.

2. **przydzielania zasobów**: istotną rolą zarządzania jest zapewnienie niezbędnych zasobów (ludzkich, systemowych i finansowych) w celu zapewnienia bezpieczeństwa zasobów informacyjnych dot. obszaru zdrowia.
3. **wybór i realizacja sposobu kontroli bezpieczeństwa**: ocena każdego z obszarów kontroli zabezpieczeń wynika bezpośrednio z normy ISO / IEC 27002 gdzie zawarte są porady i wskazówki dotyczące kontroli bezpieczeństwa w środowisku opieki zdrowotnej.
4. **kształcenie i wychowanie**: bardzo ważnym jest, aby opracowano i realizowano wymagania dotyczące szkoleń i edukacji dla wszystkich pracowników, wykonawców, służby zdrowia i innych, którzy mają dostęp do systemów informatycznych przetwarzających dokumentację medyczną i osobiste Informacje na temat zdrowia.
5. **zarządzanie SZBI**: właściwa eksploatacja SZBI jest niezbędna, jeśli poufność, integralność i dostępność systemów informatycznych i informacyjnych systemów zdrowia ma być utrzymana.
6. **zarządzanie zasobami**: efektywna ochrona informacji może być kosztowna, a kompetentne zasoby ludzkie ograniczone. Skuteczne określenie priorytetów przez najwyższy szczebel kierownictwa oraz zaangażowanie niezbędnych zasobów ludzkich ma na celu zapewnienie bieżącej działalności.
7. **zarządzanie incydentami bezpieczeństwa**: w celu zminimalizowania skutków incydentu bezpieczeństwa, ważne jest, że incydent ma być wykryty odpowiednio i że należy podjąć działania naprawcze. Procedury postępowania w przypadku wystąpienia incydentów związanych z naruszeniem bezpieczeństwa informacji muszą być poddawane regularnym przeglądom. Szczególnie ważne jest określenie obowiązków i sposobu działania w początkowej fazie reakcji, jako że zdarzenia rozwijają się szybko i krytyczny charakter systemów informacji zdrowotnej pozostawia niewiele czasu na reakcję. Przejrzyste procedury raportowania o zdarzeniach bezpieczeństwa są bardzo istotne, ponieważ regulują sposoby informowania o zdarzeniach i ich skutkach.

5.2. Przywództwo

Podmiot odpowiedzialny za bezpieczeństwo przetwarzania dokumentacji medycznej powinien wyznaczyć odpowiednie struktury, odpowiedzialne realizację poszczególnych procesów.

Najważniejszym jest przejawianie zaangażowanie wśród najwyższego kierownictwa charakteryzujące się między innymi:

a) stosowaniem się do zapisów zawartych w Polityce Bezpieczeństwa,
b) zapewnieniem sił i środków niezbędnych do zarządzania bezpieczeństwem informacji,
c) skutecznym zarządzaniem bezpieczeństwem informacji w zakresie zgodności a obowiązującymi regulacjami prawnymi oraz normami,

d) kierowaniem i wspieraniem osób przyczyniających się do osiągnięcia skuteczności Systemu Zarządzania Bezpieczeństwem Informacji,
e) promowaniem ciągłego doskonalenia i podnoszeniem świadomości.

5.3. Identyfikacja wymagań zewnętrznych i wewnętrznych dotyczących bezpieczeństwa przetwarzanych informacji

Rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny być adekwatne do jego profilu ryzyka i specyfiki działalności oraz pozwalać na efektywną realizację działań w tych obszarach.

Podmiot odpowiedzialny za przetwarzanie informacji powinien zapewnić, aby struktura organizacyjna w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego pozwalała na efektywną realizację celów w tych obszarach, odpowiednio do skali i profilu działalności oraz stopnia złożoności środowiska teleinformatycznego.

Adekwatność tej struktury powinna być systematycznie weryfikowana i w przypadku wystąpienia takiej potrzeby dostosowywana do zmian w środowisku wewnętrznym i jego otoczeniu.

W związku z powyższym precyzyjnie należy zdefiniować obowiązki i uprawnienia poszczególnych pracowników w zakresie technologii informacyjnej i bezpieczeństwa informacji. Określenie zakresów obowiązków i uprawnień powinno mieć formę pisemną, a podział obowiązków powinien minimalizować ryzyko błędów i nadużyć w procesach i systemach. W tym celu należy zwrócić uwagę na odpowiednią separację obowiązków pracowników, w szczególności oddzielenie:

a) funkcji tworzenia lub modyfikowania systemów informatycznych od ich testowania (poza testami realizowanymi przez programistów w ramach wytwarzania oprogramowania), administracji i użytkowania,
b) funkcji administrowania danym komponentem środowiska teleinformatycznego od projektowania związanych z nim mechanizmów kontrolnych w zakresie bezpieczeństwa,
c) funkcji administrowania danym systemem informatycznym od monitorowania działań jego administratorów, – funkcji audytu od pozostałych funkcji w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

W organizacji powinny zostać wyznaczone osoby lub funkcje odpowiedzialne za podejmowanie decyzji w zakresie poszczególnych systemów eksploatowanych (często zwane właścicielami systemów), opartych zarówno na infrastrukturze teleinformatycznej, jak i infrastrukturze zapewnianej przez podmioty zewnętrzne.

Do obowiązków tych osób lub funkcji powinno należeć w szczególności:

a) zapewnienie prawidłowości działania i bezpieczeństwa systemu pod względem biznesowym (np. poprzez właściwe zdefiniowanie procedur korzystania z systemu,

b) udział w procesie zarządzania ciągłością jego działania, udział w procesie zarządzania uprawnieniami),
c) nadzór nad działaniami użytkowników systemu,
d) udział w procesie podejmowania decyzji w zakresie rozwoju tych systemów.

Należy pamiętać, że zapewnienie bezpieczeństwa informacji przetwarzanych w środowisku teleinformatycznym nie jest wyłącznie domeną komórek odpowiedzialnych za obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, ale w dużej mierze zależy od właściwego postępowania bezpośrednich użytkowników systemów informatycznych i danych.

W związku z tym, każdy pracownik powinien być świadomy, że jego obowiązkiem jest dbanie o bezpieczeństwo informacji przetwarzanych w środowisku teleinformatycznym. W tym celu powinny być podejmowane działania mające na celu tworzenie tzw. kultury bezpieczeństwa informacji, edukować pracowników w zakresie bezpieczeństwa środowiska teleinformatycznego oraz uzyskać pisemne zobowiązania do przestrzegania regulacji wewnętrznych dotyczących tego obszaru oraz zapewnić pracownikom regularne szkolenia (adekwatnie do specyfiki zajmowanego przez nich stanowiska), promować zdobywanie wiedzy oraz umożliwiać im wymianę doświadczeń (np. poprzez dostęp do tzw. baz wiedzy, udział w konferencjach i forach branżowych).

5.4. Polityka bezpieczeństwa informacji i określenie celów bezpieczeństwa

W organizacji odpowiadającej za przetwarzanie dokumentacji medycznej w tym danych osobowych wrażliwych, powinien funkcjonować sformalizowany, skuteczny system zarządzania bezpieczeństwem informacji i środowiska teleinformatycznego, obejmujący działania związane z identyfikacją, szacowaniem, kontrolą, przeciwdziałaniem, monitorowaniem i raportowaniem ryzyka w tym zakresie, zintegrowany z całościowym systemem zarządzania ryzykiem i bezpieczeństwem informacji.

Podstawowym dokumentem w tym zakresie powinna być polityka bezpieczeństwa informacji.

Opisany w polityce system zarządzania bezpieczeństwem środowiska teleinformatycznego powinien wynikać ze strategii organizacji w obszarze bezpieczeństwa środowiska teleinformatycznego i być oparty o sformalizowane regulacje wewnętrzne.

System zarządzania bezpieczeństwem środowiska teleinformatycznego powinien być przedmiotem systematycznych przeglądów, mających na celu wprowadzenie ewentualnych usprawnień oraz uwzględnienie w nim zmian zachodzących zarówno w otoczeniu organizacji, jak i w jego środowisku wewnętrznym.

Powinna zostać zapewniona możliwie ścisła integracja systemu zarządzania bezpieczeństwem środowiska teleinformatycznego z systemem zarządzania ryzykiem operacyjnym. W tym celu powinno się m.in. wykorzystywać w systemie zarządzania bezpieczeństwem środowiska teleinformatycznego

stosowane narzędzia zarządzania ryzykiem operacyjnym, takie jak narzędzia oparte o czynniki otoczenia gospodarczego i kontroli wewnętrznej, samoocena ryzyka operacyjnego, analizy scenariuszowe czy mapy ryzyka.

5.5. Identyfikacja ryzyka i analiza zagrożeń dla informacji zdrowotnej

Celem identyfikacji ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego jest określenie związanych z nim zagrożeń mogących spowodować naruszenie atrybutów bezpieczeństwa przetwarzania informacji oraz określenie gdzie, w jaki sposób i dlaczego te zagrożenia mogą się zmaterializować. Identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego powinna być dokonywana systematycznie i opierać się na:

a) identyfikacji ryzyka związanego z potencjalnym naruszeniem bezpieczeństwa środowiska teleinformatycznego przed zmaterializowaniem się danych zagrożeń,
b) identyfikacji ryzyka związanego z naruszeniami bezpieczeństwa środowiska teleinformatycznego po zmaterializowaniu się zagrożeń.

Identyfikując ryzyko związane z potencjalnym naruszeniem bezpieczeństwa środowiska teleinformatycznego przed zmaterializowaniem się danych zagrożeń, szczególną uwagę powinno się poświęcić identyfikacji istniejących podatności środowiska teleinformatycznego (w tym komponentów infrastruktury teleinformatycznej) oraz zagrożeń, które mogą je wykorzystać. W tym celu powinno się przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego i stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wykorzystania automatycznych narzędzi pozwalających na identyfikację istniejących podatności.

Niezależnie od okresowej oceny, identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego powinna być przeprowadzana każdorazowo w przypadku planowania istotnych zmian, zarówno w samych systemach informatycznych, jak i w ich wykorzystaniu, a także w przypadku planów wdrożenia nowych technologii.

Identyfikując ryzyko związane z naruszeniami bezpieczeństwa środowiska teleinformatycznego po zmaterializowaniu się zagrożeń, powinno się gromadzić informacje o zaistniałych zdarzeniach mających wpływ na bezpieczeństwo przetwarzanych informacji.

Szacowanie ryzyka[30] w zakresie bezpieczeństwa środowiska teleinformatycznego ma na celu określenie prawdopodobieństwa i potencjalnego wpływu zmaterializowania się zagrożeń związanych z tym ryzykiem oraz dokonanie oceny tego ryzyka. Działania w zakresie szacowania ryzyka powinny być realizowane z uwzględnieniem klasyfikacji informacji i systemów informatycznych. Badanie wpływu

[30] PN-ISO/IEC 27005:2014 Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji

zidentyfikowanych zagrożeń powinno obejmować również elementy powiązane z komponentem, dla którego zidentyfikowano dane zagrożenie.

W wyniku przeprowadzenia szacowania ryzyka powinno się uzyskać wiedzę na temat występujących zagrożeń związanych z bezpieczeństwem środowiska teleinformatycznego, prawdopodobieństwa wystąpienia zidentyfikowanych zagrożeń oraz możliwych skutków zmaterializowania się tych zagrożeń. Wiedza ta powinna pozwolić na podjęcie właściwych decyzji w zakresie kontroli i przeciwdziałania ryzyku.

Ocena ryzyka jest mechanizmem, zgodnie z którym przeprowadzana jest kontrola zidentyfikowanych zagrożeń i badany jest wpływ zmaterializowania się ich na procesy w organizacji. Proces ten jest dobrze udokumentowany w normie ISO / IEC 27005. Ryzyko składa się ze związku przyczynowego pomiędzy występującymi źródłami ryzyka a organizacją. Wartość ryzyka jest ustalana na podstawie wartości poszczególnych aktywów, zagrożeń i słabych punktów.

Zarówno ISO / IEC 27001 oraz ISO / IEC 27005 definiują elementy analizy ryzyka i zarządzania nim w następujący sposób:

a) identyfikacja biznesowych aktywów, zagrożeń i słabych punktów;
b) ocenę wpływu na biznes;
c) prawdopodobieństwo zagrożenia i ocena podatności;
d) określenie poziomu ryzyka;
e) określenie zalecanych kontroli bezpieczeństwa;
f) porównanie z istniejących kontroli, umożliwiając identyfikację obszarów ryzyka rezydualnego;
a) możliwości postępowania z ryzykiem, w tym bezpośredniego zarządzania nim, redukcji, unikania, przeniesienia i zaakceptowania;
g) oceny ryzyka i postępowania z ryzykiem;
h) mapowanie decyzji podjętych na podstawie przeprowadzonych kontroli.

Wszystkie powyższe mają zastosowanie do opieki zdrowotnej, mimo że "ocena wpływu na biznes" wyraźnie obejmuje wiele różnych sektorów ochrony zdrowia.

Oprócz wymienionych powyżej, ważne jest również ustalenie zrozumienia zależności procesów biznesowych i zmapowanie ich na usługi, sprzęt, oprogramowanie i lokalizacje. Bez tego zrozumienie analizy wpływu na biznes, zrozumienie scenariuszy awarii, które są istotne będzie prawie niemożliwe. W świetle poważnych skutków wystąpienia incydentów bezpieczeństwa informacji możliwych w organizacjach opieki zdrowotnej, zrozumienie tych zależności staje się niezbędne.

Istnieje wiele aspektów związanych z bezpieczeństwem przetwarzania informacji a ryzykiem zmaterializowania się zagrożeń, które są przedmiotem analizy:

a) **wysoki poziom ryzyka**: dane medyczne i ochrona zdrowia opatrzona jest stosunkowo wysokim ryzykiem, szczególnie w dziedzinach takich jak laboratoria, oddziały ratunkowe i sale

operacyjne. Stwierdzenie niskiego ryzyka dla informacji , które przetwarzane są w takich obszarach, powinno być stanowczo kwestionowane.

b) **jakościowe, jak i ilościowe oceny ryzyka**: ocena ryzyka bezpieczeństwa informacji w opiece zdrowotnej powinna rozważać czynniki jakościowe, jak i ilościowe. Straty finansowe powinny nie być sprawą nadrzędną, ale mogą być brane pod uwagę, jeżeli mogą być nałożone wysokie kary za spowodowane zaniedbania.

c) **analiza ryzyka w procesach**: analiza ryzyka nie może zazwyczaj dotyczyć pojedynczych procesów, z wyjątkiem sytuacji, że dane medyczne mogą uczestniczyć tylko i wyłącznie w jednym określonym procesie. Jest to czynność związana z poszukiwaniem wzajemnych powiązań i relacji, tak aby ryzyko było w pełni identyfikowalne. Efektywna ocena ryzyka bezpieczeństwa informacji w ochronie zdrowia wymaga dostępności następujących umiejętności i wiedzy:
   - procesów występujących w ścieżkach leczenia pacjenta,
   - znajomość formatów danych klinicznych i zdolności do niewłaściwego wykorzystania tych danych;
   - znajomość zewnętrznych czynników środowiskowych, które mogą mieć wpływ na występowanie ryzyka;
   - informacje na temat IT oraz urządzeń medycznych, atrybuty i ich właściwości użytkowe/serwisowe/awaryjność;
   - znajomość historii incydentów i rzeczywistych scenariuszy zderzeń;
   - szczegółową wiedzę na temat architektury systemów;
   - znajomość programów zarządzania zmianą, za pomocą których możliwa jest zmiana poziomów ryzyka.

d) **analiza przyczyn powstania awarii**: przy ocenie ryzyka, należy wziąć również po uwagę zdarzenia, które miały już się wydarzyły. Definiowanie przyczyn powstania incydentów może wymagać specjalistycznej wiedzy. Pracownicy odpowiedzialni w podmiocie za zapewnienie bezpieczeństwa informacji, będą zobowiązani korzystać z ekspertów, którzy to będą w stanie zidentyfikować przyczyny awarii i określić scenariusze ich powstania.

e) **zobowiązania dotyczące zgodności**: ponieważ opieka zdrowotna jest sektorem o istotnych zobowiązań dotyczących zgodności zarówno prawnych jak i zawodowych, występuje zarządzanie ryzykiem odpowiedzialności, które są ze sobą powiązane.

5.6. Zarządzanie i postępowanie z ryzykiem

Uwzględniając wyniki dokonanego oszacowania ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego, powinno się podejmować stosowne decyzje dotyczące podejścia do poszczególnych zagrożeń, polegające na:

a) ograniczaniu ryzyka, tj. wprowadzaniu i modyfikacji istniejących organizacyjnych i technicznych mechanizmów kontrolnych w zakresie bezpieczeństwa środowiska teleinformatycznego,
b) transferze ryzyka, tj. przeniesieniu części lub całości ryzyka związanego z danym zagrożeniem na podmiot zewnętrzny, w szczególności poprzez zlecanie wykonywania czynności zewnętrznym dostawcom usług,
c) unikaniu ryzyka, tj. niepodejmowaniu działań, z którymi wiąże się dane zagrożenie,
d) akceptacji ryzyka, tj. świadomym niepodejmowaniu działań mających na celu ograniczenie prawdopodobieństwa lub skutków zmaterializowania się danego zagrożenia, wraz z ewentualnym zapewnieniem środków na pokrycie potencjalnie związanych z nim strat.

Ocena ryzyka jest środkiem umożliwiającym osiągnięcie celu jakim jest zapewnienie bezpieczeństwa informacjom zawartym w przetwarzanej dokumentacji medycznej. Zapewnienie bezpieczeństwa nie powinno być celem samym w sobie, ale często do tego się sprowadza. Jest to szczególnie prawdziwe w środowiskach o ograniczonych zasobach, takich jak te, które znajdują się w wielu organizacjach ochrony zdrowia. Zarządzanie ryzykiem odpowiada ocenie ryzyka poprzez określenie, które z kontrolowanych aktywów muszą zostać wzmocnione, które są już skutecznie chronione, oraz wobec których muszą być przeprowadzone dodatkowe kontrole w celu zmniejszenia poziomu ryzyka do dopuszczalnego poziomu. Integracja systemów informatycznych ochrony zdrowia sprawia, że zarządzanie ryzykiem w służbie zdrowia jest bardzo trudne, ponieważ podmioty odpowiedzialne za proces leczenia i ich systemy mogą działać jako samodzielne odizolowane wyspy. Ocena ryzyka w opiece zdrowotnej często budzi pytania o powierzenie informacji, własności, i odpowiedzialność za ich przetwarzanie. Efektywne zarządzanie ryzykiem musi zapewnić wyrównanie odpowiedzialności za bezpieczeństwo informacji z podmiotami odpowiedzialnymi w zakresie zarządzania ryzykiem. Aby wyraźnie rozróżnić proces zarządzania ryzykiem jako całość należy w pierwszej kolejności zidentyfikować ryzyka.

Proces "postępowania z ryzykiem" podkreśla aktywność zmniejszania ryzyka do poziomu akceptowalnego.

5.7. Incydenty bezpieczeństwa

W ramach zarządzania incydentami naruszenia bezpieczeństwa informacji powinny zostać sformalizowane zasady zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego, obejmujące ich identyfikację, rejestrowanie, analizę, priorytetyzację, wyszukiwanie powiązań, podejmowanie działań naprawczych oraz usuwanie przyczyn.

Powinny zostać opracowane regulacje wewnętrzne opisujące zasady postępowania w przypadkach wystąpień incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego, czyli m.in. awarii i przeciążeń systemów informatycznych, utraty urządzeń lub danych, błędów ludzkich skutkujących zagrożeniem dla bezpieczeństwa środowiska teleinformatycznego, naruszeń lub prób naruszeń zabezpieczeń, niekontrolowanych zmian w systemach itp.

Zakres i poziom szczegółowości powyższych regulacji powinny być adekwatne do skali i specyfiki przetwarzania informacji oraz poziomu złożoności jego środowiska teleinformatycznego. Zasady postępowania z incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego powinny w szczególności określać:

- metody i zakres zbierania informacji o incydentach,
- zakresy odpowiedzialności w obszarze zarządzania incydentami,
- sposób przeprowadzania analiz wpływu incydentów na środowisko teleinformatyczne, w tym jego bezpieczeństwo,
- zasady kategoryzacji i priorytetyzacji incydentów, uwzględniające klasyfikację informacji i systemów informatycznych związanych z danym incydentem,
- zasady wykrywania zależności pomiędzy incydentami (przykładem tego rodzaju zależności jest atak typu „Denial-of-Service" uniemożliwiający szybką identyfikację innego incydentu lub usunięcie jego przyczyn),
- zasady komunikacji, obejmujące zarówno pracowników, jak i zewnętrznych dostawców usług oraz – w przypadku istotnego narażenia na skutki danego incydentu – również innych stron trzecich, zapewniające odpowiednio szybkie powiadamianie zainteresowanych stron i podejmowanie działań, adekwatnie do poziomu istotności incydentu,
- zasady gromadzenia i zabezpieczania dowodów związanych z incydentami, które będą mogły zostać wykorzystane w ewentualnych postępowaniach sądowych (w szczególności minimalizujące ryzyko utraty takich dowodów lub ich odrzucenia ze względu na niewłaściwe zabezpieczenie danych),
- zasady dotyczące podejmowania działań naprawczych i zapobiegawczych, obejmujące w szczególności przypisanie osób odpowiedzialnych za realizację tych działań oraz monitorowanie stanu ich realizacji.

W celu m.in. umożliwienia podejmowania działań zapobiegawczych w odniesieniu do identyfikowanych problemów, powinien być prowadzony *rejestr incydentów* naruszenia bezpieczeństwa informacji, w którym przechowywane powinny być w szczególności informacje dotyczące:

- daty wystąpienia i identyfikacji incydentu,
- przyczyn zajścia incydentu,
- przebiegu incydentu,
- skutków incydentu,
- podjętych działań naprawczych.

5.8. Audyty wewnętrzne i zewnętrzne

Obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny być przedmiotem systematycznych, niezależnych audytów. Powinno się przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego i stopień narażenia

na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą powołania w ramach audytu wewnętrznego osób odpowiedzialnych za audyt obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego[31].

Osoby odpowiedzialne za przeprowadzanie audytów obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny posiadać odpowiednie kwalifikacje. Audyty powinny być przeprowadzane z wykorzystaniem uznanych standardów międzynarodowych i dobrych praktyk w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, jak np. standardy dotyczące audytowania systemów informatycznych:

- ISACA (Information Systems Audit and Control Association),
- COBIT (Control Objectives for Information and related Technology),
- GTAG (Global Technology Audit Guide) oraz GAIT (Guide to the Assessment for IT Risk),
- normy ISO (International Organization for Standardization).

Audyt obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinien być przeprowadzany regularnie oraz każdorazowo po wprowadzeniu zmian mogących znacząco wpłynąć na poziom bezpieczeństwa środowiska teleinformatycznego. Częstotliwość i zakres audytów powinny wynikać z poziomu ryzyka związanego z poszczególnymi obszarami audytowymi oraz wyników ich wcześniejszych przeglądów. Zlecanie dodatkowych audytów profesjonalnym instytucjom zewnętrznym specjalizującym się w badaniu obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego jest czynnikiem, który może wzmocnić w istotny sposób kontrolę nad ryzykiem związanym z tym obszarem. W związku z tym, powinno się przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą uzupełnienia działań audytu wewnętrznego przez audyty zewnętrzne przeprowadzane przez tego rodzaju podmioty, w szczególności w zakresie obszarów o wysokim poziomie ryzyka.

[31] PN-ISO/IEC 27001:2014 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania

[i] Art. 27. 1. Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. 2

[ii] Art. 9 ust 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)
Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

[iii] Art. 5 ust. 1 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)
Dane osobowe muszą być:
a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu");
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

[iv] Art. 89 ust. 1 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)
Przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele. Jeżeli cele te można zrealizować w drodze dalszego przetwarzania danych, które nie pozwalają albo przestały pozwalać na zidentyfikować osoby, której dane dotyczą, cele należy realizować w ten sposób.

[v] j.w

[vi] Art. 25 Ustawy o ochronie danych osobowych
1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku;
2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;
3) źródle danych;
4) prawie dostępu do treści swoich danych oraz ich poprawiania;
5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.
2. Przepisu ust. 1 nie stosuje się, jeżeli:
1) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą;
2) (uchylony)
3) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych w ust. 1 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania;
4) (uchylony)
5) dane są przetwarzane przez administratora, o którym mowa w art. 3 ust. 1 i ust. 2 pkt 1, na podstawie przepisów prawa;
6) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

[vii] Art. 26 Ustawy o ochronie danych osobowych
1. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:
1) przetwarzane zgodnie z prawem;
2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2;
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
2. Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje:
1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych;
2) z zachowaniem przepisów art. 23 i 25.

[viii] Art. 32 Ustawy o ochronie danych osobowych
1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:
1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna - jej miejsca zamieszkania oraz imienia i nazwiska;
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;
4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;
5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;
5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2;
5. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1-5, nie częściej niż raz na 6 miesięcy.

[ix] Art. 13, 14 i 15 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.
Art. 13 Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

1.Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:
a)swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
2.Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
d) informacje o prawie wniesienia skargi do organu nadzorczego;
e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
3.Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2. 4.Ust. 1, 2 i 3 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami. Artykuł 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą
1.Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, następujące informacje:
a)swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
c) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
d) kategorie odnośnych danych osobowych;
e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

2.Poza informacjami, o których mowa w ust. 1, administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:
a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
c) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
e) informacje o prawie wniesienia skargi do organu nadzorczego;
f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. 3.Informacje, o których mowa w ust. 1 i 2, administrator podaje:
a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu. 4.Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2. 5.Ust. 1– 4 nie mają zastosowania, gdy – i w zakresie, w jakim:
a) osoba, której dane dotyczą, dysponuje już tymi informacjami;
b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.
Artykuł 15 Prawo dostępu przysługujące osobie, której dane dotyczą
1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
a) cele przetwarzania;
b) kategorie odnośnych danych osobowych;
c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) informacje o prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle; h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. 2.Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46, związanych z przekazaniem.
3.Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.
4.Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.

[x] Art. 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 r. Nr 100 poz. 1024)

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:
1) daty pierwszego wprowadzenia danych do systemu;
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

[xi] art. 7 pkt 6 Ustawy o ochronie danych osobowych
Odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
a) osoby, której dane dotyczą,
b) osoby upoważnionej do przetwarzania danych,
c) przedstawiciela, o którym mowa w art. 31a,
d) podmiotu, o którym mowa w art. 31,
e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

[xii] art. 32 ust. 1 pkt 8 Ustawy o ochronie danych osobowych

wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych;

[xiii] Art. 32 ust. 1 pkt 6 Ustawy o ochronie danych osobowych

żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;

[xiv] Art. 35 Ustawy o ochronie danych osobowych

1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

2. W razie niedopełnienia przez administratora danych obowiązku, o którym mowa w ust. 1, osoba, której dane dotyczą, może się zwrócić do Generalnego Inspektora z wnioskiem o nakazanie dopełnienia tego obowiązku.

3. Administrator danych jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

[xv] Art. 16 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.

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

[xvi] Art. 19 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.

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

[xvii] art. 7 pkt 5 Ustawy o ochronie danych osobowych

Ilekroć w ustawie jest mowa o:

zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie;

[xviii] art. 32 ust. 1 pkt 6-8 Ustawy o ochronie danych osobowych

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;

7) wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację;

8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych;

[xix] art. 32 ust. 2 i 3 Ustawy o ochronie danych osobowych

2. W przypadku wniesienia żądania, o którym mowa w ust. 1 pkt 7, administrator danych zaprzestaje przetwarzania kwestionowanych danych osobowych albo bez zbędnej zwłoki przekazuje żądanie Generalnemu Inspektorowi, który wydaje stosowną decyzję.

3. W razie wniesienia sprzeciwu, o którym mowa w ust. 1 pkt 8, dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator danych może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.

[xx] Art.. 35 Ustawy o ochronie danych osobowych – wskazany powyżej

[xxi] art. 17 -19 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).

Artykuł 17 Prawo do usunięcia danych („prawo do bycia zapomnianym")

1.Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

2.Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3.Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3; d)do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub e) do ustalenia, dochodzenia lub obrony roszczeń.

Artykuł 18 Prawo do ograniczenia przetwarzania

1.Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

2.Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony

roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
3.Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.
Artykuł 19 Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania
Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

[xxii] art. 32 ust. 1 pkt. 7-8 i ust. 2-3 Ustawy o ochronie danych osobowych – wskazane powyżej

[xxiii] Art. 21 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).

1.Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
2.Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
3.Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.
4.Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1 i 2, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
5.W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.
6.Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

[xxiv] Art. 26a Ustawy o ochronie danych osobowych

1. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.
2. Przepisu ust. 1 nie stosuje się, jeżeli rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględnia wniosek osoby, której dane dotyczą, albo jeżeli zezwalają na to przepisy prawa, które przewidują również środki ochrony uzasadnionych interesów osoby, której dane dotyczą.

[xxv] art. 32 ust. 1 pkt 5a i pkt 9 oraz ust 3a Ustawy o ochronie danych osobowych

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:
5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2;
9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem art. 26a ust. 1.

[xxvi] art. 32 ust 3a Ustawy o ochronie danych osobowych

3a. W razie wniesienia żądania, o którym mowa w art. 32 ust. 1 pkt 9, administrator danych bez zbędnej zwłoki rozpatruje sprawę albo przekazuje ją wraz z uzasadnieniem swojego stanowiska Generalnemu Inspektorowi, który wydaje stosowną decyzję.

[xxvii] Art. 22 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).
1.Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:
a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.
3.W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.
4.Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.
[xxviii] Art. 36 ust. 1 i 2 Ustawy o ochronie danych osobowych
1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.
[xxix] art. 36b Ustawy o ochronie danych osobowych
W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, wykonuje administrator danych.
[xxx] Art. 37 Ustawy o ochronie danych osobowych
Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.
[xxxi] art. 36a ust. 2 pkt 1 lit. c Ustawy o ochronie danych osobowych
Do zadań administratora bezpieczeństwa informacji należy:
1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
[xxxii] art. 39 ust. 1 pkt a i b 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).
1.Inspektor ochrony danych ma następujące zadania:
a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
[xxxiii] art. 39 ust. 2 Ustawy o ochronie danych osobowych

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

[xxxiv] art. 40 Ustawy o ochronie danych osobowych

Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a.

[xxxv] art. 43 Ustawy o ochronie danych osobowych

1. Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych:

1) zawierających informacje niejawne;

1a) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności;

2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym;

2a) przetwarzanych przez Generalnego Inspektora Informacji Finansowej;

2b) przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym;

2c) przetwarzanych przez właściwe organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej;

3) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego;

4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się;

5) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta;

6) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego;

7) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności;

8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej;

9) powszechnie dostępnych;

10) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego;

11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego;

12) przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1.

1a. Obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1, nie podlega administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił go Generalnemu Inspektorowi do rejestracji, z zastrzeżeniem art. 46e ust. 2.

2. W odniesieniu do zbiorów, o których mowa w ust. 1 pkt 1 i 3, oraz zbiorów, o których mowa w ust. 1 pkt 1a, przetwarzanych przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne, Generalnemu Inspektorowi nie przysługują uprawnienia określone w art. 12 pkt 2, art. 14 pkt 1 i 3-5 oraz art. 15-18.

[xxxvi] § 3 ust. 4 Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r (Dz. U. z 2015, poz. 745)

4. Administrator bezpieczeństwa informacji w planie sprawdzeń uwzględnia, w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych:

1) z zasadami, o których mowa w art. 23–27 i art. 31–35 ustawy;

2) z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37–39 ustawy oraz przepisach wydanych na podstawie art. 39a ustawy;

3) z zasadami przekazywania danych osobowych, o których mowa w art. 47–48 ustawy;

4) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 ustawy.

[xxxvii] art. 23 Ustawy o ochronie danych osobowych

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:
1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;
2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
2. Zgoda, o której mowa w ust. 1 pkt 1, może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.
2a. Podmioty, o których mowa w art. 3 ust. 1, uważa się za jednego administratora danych, jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu.
3. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a spełnienie warunku określonego w ust. 1 pkt 1 jest niemożliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.
4. Za prawnie usprawiedliwiony cel, o którym mowa w ust. 1 pkt 5, uważa się w szczególności:
1) marketing bezpośredni własnych produktów lub usług administratora danych;
2) dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

[xxxviii] art. 27 Ustawy o ochronie danych osobowych

1. Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
2. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli:
1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych;
2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;
3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora;
4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych;
5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem;
6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;
7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;
8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;
9) jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;
10) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

[xxxix] art. 26 Ustawy o ochronie danych osobowych – wskazany wyżej
[xl] art. 26a Ustawy o ochronie danych osobowych– wskazany wyżej
[xli] art. 24 Ustawy o ochronie danych osobowych
1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:
1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku;
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
3) prawie dostępu do treści swoich danych oraz ich poprawiania;
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
2. Przepisu ust. 1 nie stosuje się, jeżeli:
1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;
2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.
[xlii] Art. 25 Ustawy o ochronie danych osobowych – wskazany wyżej
[xliii] Art. 7 pkt 5 Ustawy o ochronie danych osobowych – wskazany wyżej
[xliv] art. 32 ust. 1 pkt 1-5a Ustawy o ochronie danych osobowych
1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:
1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna - jej miejsca zamieszkania oraz imienia i nazwiska;
5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2;
[xlv] art. 33 Ustawy o ochronie danych osobowych
1. Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt 1-5a.
2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.
[xlvi] art. 34 Ustawy o ochronie danych osobowych
Administrator danych odmawia osobie, której dane dotyczą, udzielenia informacji, o których mowa w art. 32 ust. 1 pkt 1-5a, jeżeli spowodowałoby to:
1) ujawnienie wiadomości zawierających informacje niejawne;
2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego;
3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa;
4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.
[xlvii] art. 32 ust. 1 pkt 6 Ustawy o ochronie danych osobowych – wskazany powyżej

[xlviii] art. 35 Ustawy o ochronie danych osobowych – wskazany powyżej
[xlix] art. 32 ust. 1 pkt 7 art. 32 ust. 1 pkt 8 i art. 32 ust. 1 pkt 5a oraz pkt 9 Ustawy o ochronie danych osobowych – wskazane powyżej
[l] art. 40 Ustawy o ochronie danych osobowych – wskazany powyżej
[li] art. 43 Ustawy o ochronie danych osobowych – wskazany powyżej
[lii] art. 46 Ustawy o ochronie danych osobowych
1. Administrator danych może, z zastrzeżeniem ust. 2, rozpocząć ich przetwarzanie w zbiorze danych po zgłoszeniu tego zbioru Generalnemu Inspektorowi, chyba że ustawa zwalnia go z tego obowiązku.
2. Administrator danych, o których mowa w art. 27 ust. 1, może rozpocząć ich przetwarzanie w zbiorze danych po zarejestrowaniu zbioru, chyba że ustawa zwalnia go z obowiązku zgłoszenia zbioru do rejestracji.

[liii] art. 47 Ustawy o ochronie danych osobowych
1. Przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych.

1a. Odpowiedni poziom ochrony danych osobowych, o którym mowa w ust. 1, jest oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe. 2. Przepisu ust. 1 nie stosuje się, gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej, gwarantującymi odpowiedni poziom ochrony tych danych.
3. Administrator danych może jednak przekazać dane osobowe do państwa trzeciego, jeżeli:
1) osoba, której dane dotyczą, udzieliła na to zgody na piśmie;
2) przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie;
3) przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem;
4) przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych;
5) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą;
6) dane są ogólnie dostępne.

[liv] art. 48 Ustawy o ochronie danych osobowych

1. W przypadkach innych niż wymienione w art. 47 ust. 2 i 3 przekazanie danych osobowych do państwa trzeciego, które nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, może nastąpić po uzyskaniu zgody Generalnego Inspektora, wydanej w drodze decyzji administracyjnej, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.
2. Zgoda Generalnego Inspektora nie jest wymagana, jeżeli administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez:
1) standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską zgodnie z art. 26 ust. 4 dyrektywy 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 (Dz. Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.) lub
2) prawnie wiążące reguły lub polityki ochrony danych osobowych, zwane dalej „wiążącymi regułami korporacyjnymi", które zostały zatwierdzone przez Generalnego Inspektora zgodnie z ust. 3-5.
3. Generalny Inspektor zatwierdza, w drodze decyzji administracyjnej, wiążące reguły korporacyjne przyjęte w ramach grupy przedsiębiorców do celów przekazania danych osobowych przez administratora danych lub podmiot, o którym mowa w art. 31 ust. 1, do należącego do tej samej grupy innego administratora danych lub podmiotu, o którym mowa w art. 31 ust. 1, w państwie trzecim.
4. Generalny Inspektor przed zatwierdzeniem wiążących reguł korporacyjnych może przeprowadzić konsultacje z właściwymi organami ochrony danych osobowych państw należących do Europejskiego Obszaru Gospodarczego, na których terytorium mają siedziby przedsiębiorcy należący do grupy, o której mowa w ust. 3, przekazując im niezbędne informacje w tym celu.
5. Generalny Inspektor, wydając decyzję, o której mowa w ust. 3, uwzględnia wyniki przeprowadzonych konsultacji, o których mowa w ust. 4, a jeżeli wiążące reguły korporacyjne były przedmiotem rozstrzygnięcia organu ochrony danych osobowych innego państwa należącego do Europejskiego Obszaru Gospodarczego - może uwzględnić to rozstrzygnięcie.

[lv] art. 31 Ustawy o ochronie danych osobowych

1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.
2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.
2a. Nie wymaga zawarcia umowy między administratorem a podmiotem, o którym mowa w ust. 1, powierzenie przetwarzania danych, w tym przekazywanie danych, jeżeli ma miejsce między podmiotami, o których mowa w art. 3 ust. 1.

3. Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki

zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.
4. W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.
5. Do kontroli zgodności przetwarzania danych przez podmiot, o którym mowa w ust. 1, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19.
Art. 31a. W przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim, administrator danych jest obowiązany wyznaczyć swojego przedstawiciela w Rzeczypospolitej Polskiej.

[lvi] § 6 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
1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:
1) podstawowy;
2) podwyższony;
3) wysoki.
2. Poziom co najmniej podstawowy stosuje się, gdy:
1) w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 27 ustawy, oraz
2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
3. Poziom co najmniej podwyższony stosuje się, gdy:
1) w systemie informatycznym przetwarzane są dane osobowe, o których mowa w art. 27 ustawy, oraz
2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
4. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.
5. Opis środków bezpieczeństwa stosowany na poziomach, o których mowa w ust. 1, określa załącznik do rozporządzenia.

[lvii] § 5 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
Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:
1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania:
a) elektronicznych nośników informacji zawierających dane osobowe,
b) kopii zapasowych, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

[lviii] § 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

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:
1) daty pierwszego wprowadzenia danych do systemu;
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

[lix] § 7 ust. 1 pkt 4 j.w

[lx] § 7 ust. 1 j.w

[lxi] § 4.i 5 Rozporządzanie 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

§ 4. Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:
1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4) sposób przepływu danych pomiędzy poszczególnymi systemami;
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
§ 5. Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:
1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania:
a) elektronicznych nośników informacji zawierających dane osobowe,
b) kopii zapasowych, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

[lxii] art. 7 pkt 6 Ustawy o ochronie danych osobowych – wskazany wyżej

[lxvi] Art. 17 ust.. 3 dyrektywy 95/46/We Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych *Przetwarzanie danych przez przetwarzającego musi być regulowane przez umowę lub akt prawny, na mocy których przetwarzający podlega administratorowi danych i które w szczególności postanawiają, że:*
— przetwarzający działa wyłącznie na polecenie administratora danych,
— obowiązki wymienione w ust. 1, określone przez ustawodawstwo Państwa Członkowskiego, w którym przetwarzający prowadzi działalność gospodarczą, dotyczą również przetwarzającego.
[lxvii] Art. 31 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.
[lxviii] art. 28 ust. 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)
1.Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
2.Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
3.Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:
a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmuje wszelkie środki wymagane na mocy art. 32;
d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4; e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;
f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;
g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.
W związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

4.Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający

korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.
5.Wystarczające gwarancje, o których mowa w ust. 1 i 4 niniejszego artykułu, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.
6.Bez uszczerbku dla indywidualnych umów między administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, o których mowa w ust. 3 i 4 niniejszego artykułu, mogą się opierać w całości lub w części na standardowych klauzulach umownych, o których mowa w ust. 7 i 8 niniejszego artykułu, także gdy są one elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43.
7.Komisja może określić standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.
8.Organ nadzorczy może przyjąć standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z mechanizmem spójności, o którym mowa w art. 63.
9.Umowa lub inny akt prawny, o których mowa w art. 3 i 4, mają formę pisemną, w tym formę elektroniczną.
10.Bez uszczerbku dla art. 82, 83 i 84, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

[lxix] art. 27 ust. 2 pkt 7 Ustawy o ochronie danych osobowych
Przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych.

[lxx] art. 24 ust. 4 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2016 nr 0 poz. 186)
Podmiot udzielający świadczeń zdrowotnych może zawrzeć umowę, o której mowa w art. 31 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135), pod warunkiem zapewnienia ochrony danych osobowych oraz prawa do kontroli przez podmiot udzielający świadczeń zdrowotnych zgodności przetwarzania danych osobowych z tą umową przez podmiot przyjmujący te dane.

[lxxi] Art. 24 ust 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2016 nr 0 poz. 186)
Osoby wykonujące zawód medyczny oraz inne osoby, wykonujące 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, są uprawnione do przetwarzania danych zawartych w dokumentacji medycznej, o której mowa w art. 25, w celu ochrony zdrowia, udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, utrzymania systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna i zapewnieniem bezpieczeństwa tego systemu.

[lxxii] Art. 40 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)
Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu niniejszego rozporządzenia – z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

[lxxiii] Art. 42 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)

Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Przy tym uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

[lxxiv] art. 36 ust. 1 Ustawy o ochronie danych osobowych – wskazany wyżej

[lxxv] artykuł 10 Dyrektywy 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

Państwa Członkowskie zapewniają, aby administrator danych lub jego przedstawiciel miał obowiązek przedstawienia osobie, której dane dotyczą i od której gromadzone są dane, conajmniej następujących informacji, z wyjątkiem przypadku, kiedy informacje takie już posiada:

a) tożsamości administratora danych i ewentualnie jego przedstawiciela;

b) celów przetwarzania danych, do których dane są przeznaczone;

c) wszelkich dalszych informacji, jak np.:

— odbiorcy lub kategorie odbierających dane,

— tego, czy odpowiedzi na pytania są obowiązkowe czy dobrowolne oraz ewentualne konsekwencje nieudzielenia odpowiedzi,

— istnienie prawa wglądu do swoich danych oraz ich sprostowania, o ile takie dalsze informacje są potrzebne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku doosoby, której dane dotyczą.

[lxxvi] art. 13 i 14 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. – wskazane wyżej

[lxxvii] art. 17 ust. 2 Dyrektywy 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

Państwa Członkowskie zobowiązują administratora danych ,w przypadku przetwarzania danych w jego imieniu, do wybrania przetwarzającego, o wystarczających gwarancjach odnośnie do technicznych środków bezpieczeństwa oraz rozwiązań organizacyjnych, regulujących przetwarzanie danych, oraz zapewnienia stosowania tych środków i rozwiązań.

[lxxviii] § 6 ust. 1 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 – wskazany powyżej

[lxxix] art. 27 Ustawy o ochronie danych osobowych – wskazany wyżej

[lxxx] art. 25 ust. 1 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.

Artykuł 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych 1.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 wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

[lxxxi] art. 32 ust. 1 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.

Artykuł 32 Bezpieczeństwo przetwarzania 1.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, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku: a) pseudonimizację i szyfrowanie danych osobowych; b)zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

[lxxxii] art. 36 ust. 1 Ustawy o ochronie danych osobowych – wskazany wyżej

[lxxxiii] art. 27 ust. 1 Ustawy o ochronie danych osobowych – wskazany wyżej