**KODEKS POSTĘPOWANIA DOTYCZĄCY OCHRONY DANYCH OSOBOWYCH PRZETWARZANYCH
W MAŁYCH PLACÓWKACH MEDYCZNYCH**

****

****

1. **WSTĘP**

**Jakie są cele kodeksu postępowania dla MPM?**

Niniejszy dokument stanowi kodeks postępowania w rozumieniu art. 40 ogólnego rozporządzenia o ochronie danych (RODO)[[1]](#footnote-1). Głównym celem kodeksu jest zatem doprecyzowanie zasad ochrony danych zawartych w RODO i podniesienie poziomu ochrony danych osobowych przez Małe Placówki Medyczne (MPM). Na potrzeby kodeksu, przez MPM rozumie się podmioty wykonujące działalność leczniczą[[2]](#footnote-2) – placówki podstawowej opieki zdrowotnej i poradnie specjalistyczne.

Kodeks został opracowany dla MPM, które administrują danymi zawierającymi informacje o stanie zdrowia osób fizycznych, aby wesprzeć MPM we właściwym wdrożeniu przepisów RODO.

Dokument zawiera praktyczne wskazówki dotyczące realizacji konkretnych obowiązków wynikających z RODO, uwzględniające specyfikę funkcjonowania MPM
– w szczególności branżowe przepisy regulujące działalność leczniczą. Sektorowe zorientowanie wytycznych zawartych w kodeksie pozwoli na dopasowanie ich
do oczekiwań i praktyki sektora małych placówek medycznych oraz umożliwi łatwiejsze i skuteczniejsze wdrożenie i stosowanie przepisów RODO.

Niniejszy kodeks ma również na celu zwiększenie zaufania pacjentów do MPM
i gwarancję, że placówki, które przystępują do kodeksu, zapewniają bezpieczeństwo danych osobowych na odpowiednio wysokim poziomie poprzez stosowanie odpowiednich zasad i instrumentów prawnych ochrony danych przy uwzględnieniu ryzyka dla praw i wolności pacjentów wynikającego z przetwarzania ich danych osobowych.

Kodeks ma zastosowanie jedynie do danych osobowych przetwarzanych w związku działalnością leczniczą MPM. Dokument nie dotyczy przetwarzania danych osobowych pracowników, współpracowników oraz kandydatów do pracy w MPM.

Mała Placówka Medyczna w rozumieniu niniejszego kodeksu jest administratorem danych, co oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Dane osobowe oznaczają z kolei wszelkie informacje
o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej[[3]](#footnote-3).

**Dlaczego kodeks postępowania dla MPM jest potrzebny?**

RODO zmienia sposób, w jaki musimy myśleć o prywatności. Nie od dziś wiadomo,
że niewłaściwe przetwarzanie danych osobowych może wiązać się z bardzo poważnymi konsekwencjami dla osób, których te dane dotyczą. W obliczu dynamicznego rozwoju nowych technologii konsekwencje naruszeń bezpieczeństwa danych są coraz większe. Dlatego RODO nakazuje systematyczną analizę ryzyka wystąpienia tych negatywnych konsekwencji, jakie wiąże się z przetwarzaniem danych osobowych. To powoduje,
że ochrona danych osobowych musi być procesem żywym, stale monitorowanym
i poprawianym – tak by zastosowane środki bezpieczeństwa zawsze odpowiadały zmieniającym się wyzwaniom i zagrożeniom.

Wobec powyższego, na szczególną ochronę zasługują dane wrażliwe (nazywane
w RODO danymi szczególnej kategorii), jakimi są m.in. informacje dotyczące stanu zdrowia. Są to dane wprost przypisane do konkretnych osób i niezmienne. Konsekwencje dostania się takich informacji w niepowołane ręce mogą być bardzo niekorzystne. Ważne jest zatem, by wszyscy administratorzy danych, którzy wykorzystują dane wrażliwe, posiadali odpowiednią wiedzę na temat ich ochrony
i świadomość potencjalnych rodzajów ryzyka, jakie wiążą się z niewłaściwym wykorzystaniem takich danych.

Dlatego też wszystkie operacje na danych, takie jak: zbieranie, przechowywanie, usuwanie, opracowywanie, udostępnianie, powinny opierać się na zasadach ochrony danych, odzwierciedlających podstawowe wartości RODO:

– **Zasada rzetelności i legalności.** Zasada ta wymaga, by dane przetwarzano uczciwie
i zgodnie z prawem. MPM zapewnia, że dane osobowe przetwarza w zgodzie z RODO (poprzez zapewnienie podstaw prawnych przetwarzania danych i realizację praw pacjentów) oraz wszystkimi przepisami regulującymi funkcjonowanie tego podmiotu.

– **Zasada przejrzystości.** Przetwarzanie danych osobowych powinno być więc zrozumiałe dla osób, których dane są przetwarzane. MPM uwzględnia zatem potrzeby
i oczekiwania pacjentów oraz komunikuje się z nimi w jasny i zrozumiały sposób.

– **Zasada ograniczenia celu.** Zasada ta wymaga, by wszystkie dane osobowe gromadzić w oznaczonych celach i by nie przetwarzać ich w sposób niezgodny w tymi celami. Określenie celu ustanawia ramy, których administrator danych przekroczyć nie może. MPM nie zbiera danych „na zapas”, dla przyszłych nieoznaczonych jeszcze celów. Podkreślić jednocześnie należy, że nie jest zbieraniem „na zapas” gromadzenie informacji o stanie zdrowia w trakcie wywiadu medycznego – jest to uzasadnione wymogami medycyny i koniecznością udzielenia pacjentowi niezbędnej pomocy.

– **Zasada minimalizacji danych.** Zebrane dane muszą być adekwatne do celu, który administrator chce osiągnąć. Zasada ta wymaga, by pozyskiwać jedynie te dane, które
są niezbędne do realizacji celu. MPM nie dopuszcza zatem sytuacji, kiedy zbiera się takie dane, które jedynie potencjalnie mogą zostać użyte w przyszłości. Wszystkie dane niezbędne dla prawidłowej diagnozy i procesu leczenia, nawet jeśli mają posłużyć do jego osiągnięcia w przyszłości (w tym dane zebrane podczas wywiadu medycznego), będą jednak poprawne. MPM zapewnia również, że zasada minimalizacji danych uwzględniona będzie również we wszystkich procesach tworzenia nowych produktów, usług i systemów, tak by domyślnie ograniczać ilość zbieranych danych, zakres ich przetwarzania oraz okres ich przechowywania.

– **Zasada poprawności danych**. Zgodnie z tą zasadą wszelkie dane osobowe powinny być prawidłowe i aktualne. MPM podejmuje więc starania by informacje, które przetwarza były zgodne z prawdą i uaktualniane, a w razie potrzeby usunięte
lub sprostowane. W praktyce oznacza to, że kiedy MPM dowiaduje się o zmianie danych, powinien niezwłocznie ten fakt odnotować w swoich bazach i dokumentacji.

– **Zasada ograniczenia przetwarzania.** Zgodnie z nią MPM nie przechowuje danych przez okres dłuższy niż jest to niezbędne do realizacji celu, dla którego dane te zostały zebrane. To cel przetwarzania decyduje zatem o długości przechowywania danych. Oczywiście zdarzają się sytuacje uzasadniające dalsze ich przechowywanie,
np. do celów archiwalnych. W praktyce funkcjonowania MPM okres przechowywania danych będzie ściśle określony przepisami regulującymi przechowywanie dokumentacji medycznej.

– **Zasada integralności i poufności.** MPMdba o bezpieczeństwo danych osobowych
i przetwarza dane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym, np. poprzez stosowanie szyfrowania danych oraz zapewniający ochronę przed przypadkową utratą, zniszczeniem lub uszkodzeniem,.

– **Zasada rozliczalności.** Zgodnie z tą zasadą, MPM odpowiada za przestrzeganie wszystkich powyższych zasad i jest w stanie to wykazać. Rozliczalność oznacza wdrożenie odpowiednich środków gwarantujących wysoki poziom ochrony danych oraz sporządzenie stosownej dokumentacji pokazującej, w jaki sposób przestrzegane
są obowiązki wynikających z RODO. **Niniejszy kodeks może pomóc w wykazaniu przez MPM przestrzegania przepisów RODO, a jego stosowanie może posłużyć za element wykazujący wywiązywanie się MPM z obowiązków nałożonych przez RODO na administratorów danych.** W niniejszym dokumencieprzekazane są bowiem wskazówki co do tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie przepisów prawa.

**Kto może przystąpić do kodeksu?**

Kodeks został stworzony przez Federację Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie”, przy udziale ekspertów ochrony danych
z Jamano Sp. z o.o. Kodeks uwzględnia również uwagi podmiotów zainteresowanych,
z którymi dokument konsultowano, m.in. *Fundacja Panoptykon.*

Kodeks ma zastosowanie do MPM będących członkami struktur regionalnych Federacji. W celu przystąpienia do stosowania kodeksu, MPM składa do Zarządu Federacji pisemną deklarację przystąpienia zawierającą przyjęcie zobowiązania
do przestrzegania zasad i postanowień w nim zawartych. Jedynie te placówki, które zgłoszą Zarządowi Federacji stosowną deklarację, mogą powoływać się na stosowanie postanowień niniejszego kodeksu w celu wykazywania zgodności z RODO.

Zarząd Federacji stale monitoruje przestrzeganie postanowień kodeksu w placówkach, które zdecydowały się do niego przystąpić. W tym celu Zarząd może zdecydować
o wyznaczeniu dedykowanego zespołu kontrolującego. W uzasadnionych wypadkach Zarząd Federacji może zdecydować o zawieszeniu bądź wykluczeniu placówki w grupy stosującej kodeks. Zarząd Federacji przyznaje również takie uprawnienia podmiotowi monitorującemu, o którym mowa w art. 41 RODO.

|  |
| --- |
| ***Podstawy prawne RODO:******Artykuł 5 Zasady dotyczące przetwarzania danych osobowych****1. 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").**2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").* |

1. **PRZETWARZANIE DANYCH OSOBOWYCH ZGODNIE Z PRAWEM**

## **Jakie są podstawy prawne przetwarzania danych osobowych przez MPM?**

Przepisy RODO określają katalog przesłanek, które legalizują przetwarzanie danych.
W praktyce funkcjonowania MPM będzie mogła przetwarzać dane osobowe pacjentów jeśli:

- jest to niezbędne do celów profilaktyki zdrowotnej i zapewnienia opieki zdrowotnej
na podstawie odpowiednich przepisów prawa;

- pacjent wyraził zgodę na przetwarzanie jego danych osobowych;

- MPM posiada prawnie uzasadniony interes w przetwarzaniu danych.

Artykuł 25 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta określa minimalną zawartość dokumentacji medycznej, wskazując jakie dane osobowe pacjenta można przetwarzać: imię i nazwisko, datę urodzenia, oznaczenie płci, adres miejsca zamieszkania, numer PESEL oraz imię i nazwisko przedstawiciela ustawowego osoby małoletniej. Zbieranie tych danych znajduje zatem uzasadnienie w przepisie prawa i pacjent jest zobowiązany do przekazania tych danych MPM.

Pacjent MPM może wyrazić zgodę na przesyłanie newslettera pod wskazany
w oświadczeniu pacjenta adres e-mail, w którym placówka medyczna informuje
o najnowszych informacjach dotyczących placówki. Przesyłanie informacji marketingowych MPM będzie zatem możliwe jedynie po uzyskaniu zgody pacjenta.

MPM może pozyskiwać i wykorzystywać dane osobowe także dla potrzeb obrony przed roszczeniami, w szczególności związanymi z udzielonymi świadczeniami zdrowotnymi.

Wszystkie te przesłanki mają charakter autonomiczny, co oznacza, że MPM może przetwarzać dane po spełnieniu wyłącznie jednej z nich. W praktyce oznacza to, że MPM nie zbiera dodatkowych zgód na przetwarzanie danych osobowych jeśli ma już prawo do przetwarzania danych osobowych na podstawie konkretnego przepisu prawa.

## **Kiedy przepis prawa będzie podstawą do przetwarzania danych?**

MPM przetwarza dane o stanie zdrowia swoich pacjentów, natomiast w przepisach RODO znajdziemy ogólną podstawę do przetwarzania danych szczególnej kategorii. Jest to art. 9 ust. 2 lit. h., który stanowi postawę przetwarzania niezbędnego m.in. do celów profilaktyki zdrowotnej lub medycyny pracy oraz zapewnienia opieki zdrowotnej. Przepis ten nie stanowi samodzielnej podstawy prawnej, ale jedynie w połączeniu
z odpowiednim przepisem polskiego prawa.

Bezpośrednia podstawa prawna przetwarzania musi być natomiast przewidziana
w przepisach krajowych, powszechnie obowiązujących. Należy szukać zatem stosownych przepisów polskich ustaw i rozporządzeń odnoszących się do szeroko rozumianego obszaru medycznego. Wśród nich można wymienić:

* ustawę o prawach pacjenta i Rzeczniku Praw Pacjenta,
* ustawę o działalności leczniczej,
* ustawę o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych,
* ustawę o systemie informacji w ochronie zdrowia,
* ustawę o podstawowej opiece zdrowotnej,
* ustawę o zawodach lekarza i lekarza dentysty,
* ustawę o służbie medycyny pracy,
* ustawę o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi,
* ustawę o leczeniu niepłodności.

W tych przepisach MPM znajdzie co do zasady jasne i precyzyjnie wskazanie celu przetwarzania, rodzaj danych, które można zbierać oraz okresy przechowywania tych danych. Wszelkie rozważania dotyczące zasady ograniczonego celu i minimalizacji danych, poczynione wcześniej, będą miały szczególne zastosowanie do tej sytuacji.

Z uwagi na szczególny charakter danych dotyczących zdrowia, przepisy RODO przewidują również, że dane te mogą być przetwarzane wyłącznie przez pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej lub inną osobę podlegającą obowiązkowi zachowania tajemnicy zawodowej.

Przepisy prawa są również podstawą do wysyłania zaproszeń na badania z zakresu profilaktyki zdrowotnej oraz zbierania danych o stanie zdrowia niezbędnych
do realizacji badań profilaktycznych. Wskazane powyżej przepisy obejmują pojęciem świadczeń zdrowotnych działania służące zachowaniu, ratowaniu, przywracaniu
lub poprawie zdrowia oraz inne działania medyczne wynikające z procesu leczenia
lub przepisów odrębnych regulujących zasady ich udzielania, jak również działania służące profilaktyce zdrowotnej. Wykorzystywanie danych pacjentów do wysyłki zaproszeń do udziału w badaniach profilaktycznych mieści się w ramach dozwolonej promocji zdrowia. Pamiętać jednak należy, że owa promocja zdrowia powinna
być wykonywana przez MPM wyłącznie w zakresie wykonywanych przez nie świadczeń zdrowotnych.

**W jakich celach MPM może zbierać zgody na przetwarzanie danych?**

Jak już wspomniano, przetwarzanie danych pacjenta na podstawie zgody jest możliwe do celów niemedycznych, o czym powyżej. W praktyce funkcjonowania MPM zgoda będzie najczęściej podstawą przetwarzania do celów marketingowych, w tym wysyłania newsletterów czy innych form reklamy (np. promocja nowych usług MPM).

Pozyskanie odrębnej zgody pacjenta będzie również zasadne w wypadku prowadzenia badań poziomu zadowolenia pacjentów z usług świadczonych przez MPM, kiedy do pacjentów wysyłane są ogólne ankiety z pytaniami o poziom
ich satysfakcji z usług MPM. Zgoda nie będzie potrzebna w sytuacji, kiedy ankiety są anonimowe (nie zbierane są żadne dane mogące posłużyć do identyfikacji konkretnego pacjenta przez MPM, a pytania przygotowane są na takim poziomie ogólności, który uniemożliwiaja taką identyfikację) lub też są narzędziem do badania jakości udzielonych pacjentowi świadczeń zdrowotnych (w takiej sytuacji dane zebrane dla celów medycznych mogą również posłużyć do przeprowadzenia takiego badania jakości).

Możliwa będzie również zgoda pacjenta na przekazania jego danych w celu prowadzenia badań naukowych. Należy wówczas pamiętać, że taka zgoda powinna być wyraźnym oświadczeniem pacjenta, które nie będzie pozostawiało wątpliwości, na co pacjent się zgadza.

MPM prosi o wyraźną zgodę pacjenta na przekazanie jego dokumentacji medycznej do eksperta z biobanku, do którego MPM zwraca się o dokonanie analizy naukowej. Z uwagi na szczególny charakter tych informacji MPM prosi
o podpis osobę, której dane dotyczą, w celu uzyskania ważnej wyraźnej zgody oraz aby móc później wykazać, że uzyskano wyraźną zgodę tego pacjenta.

## **Jak należy zbierać zgody na przetwarzanie danych?**

Zgodnie z RODO taka zgoda może zostać wyrażona przez pacjenta poprzez złożenie oświadczenia ustnie lub pisemnie, a także przez wyraźne działanie potwierdzające. Wyrażenie zgody powinno nastąpić przed faktycznym rozpoczęciem przetwarzania.

Działanie potwierdzające oznacza, że pacjent musiał podjąć celowe działanie
w celu wyrażenia zgody. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej lub wysłanie pod wskazany adres maila,
czy też pozostawienie swojej wizytówki podczas organizacji loterii z nagrodami.

Niedopuszczalne będą natomiast wszelkie modele pozyskiwania zgody opierające się na milczeniu, bierności czy nieuwadze pacjenta. Ważną zgodą nie będzie zatem zignorowanie przez osobę domyślnie zaznaczonego okienka, jak również wykorzystanie przez MPM z opcji domyślnych, które osoba musi zmienić, aby odmówić przetwarzania danych.

Bardzo ważnym aspektem w kontekście zasady rozliczalności jest konieczność udowodnienia, że pacjent wyraził na to świadomie zgodę. Dobrą praktyką będzie zatem dokumentowanie czynności związanych z pozyskiwaniem zgód, np. rejestrowanie zgód udzielonych ustnie lub ewidencjonowanie oświadczeń o wyrażeniu zgody. Wszystko
po to, aby wykazać, w jaki sposób i kiedy uzyskano zgodę oraz jakie informacje pacjent otrzymał w momencie uzyskiwania zgody.

## **Jakie warunki MPM musi spełnić by zgoda była ważna?**

Aby zgoda była ważna, oświadczenie lub działanie potwierdzające musi być dobrowolne, konkretne, świadome i jednoznaczne. Jak podkreśla Prezes Urzędu Ochrony Danych Osobowych[[4]](#footnote-4) (PUODO, do 25 maja 2018 r. GIODO) kryteria
te oznaczają[[5]](#footnote-5):

**dobrowolność** – możliwość realnego, swobodnego wyboru, bez jakiegokolwiek przymusu; brak zgody nie może również powodować negatywnych konsekwencji
dla osoby, której dane dotyczą; MPM dba, by pozyskiwane zgody nie były wymuszone, tj. nie mogą być przedkładane do podpisu jako konieczny element realizacji świadczenia medycznego (np. zgoda na przetwarzanie danych osobowych zawarta na deklaracji wyboru).

**konkretność** – precyzyjne określenie celu przetwarzania danych oraz zakresu danych; niedopuszczalne jest zbieranie zgód blankietowych, ogólnych; należy również wyraźnie oddzielić informacje związane z uzyskiwaniem zgody od informacji dotyczących innych kwestii; MPM w klauzuli zgody wskazuje nazwę i adres administratora oraz cele przetwarzania.

**świadomość** – przed uzyskaniem zgody należy osobom, których dane dotyczą, zapewnić niezbędne informacje do podjęcia świadomej decyzji i zrozumienia,
na co wyrażają zgodę; prosząc o zgodę, MPM powinien używać jasnego
i prostego języka, zrozumiałego dla pacjenta;

**jednoznaczność** – ważna zgoda musi być jednoznacznie potwierdzona oświadczeniem na piśmie lub przez wyraźne działanie potwierdzające, co oznacza, że dana osoba musi podjąć celowe działanie w celu wyrażenia zgody na określone przetwarzanie.
MPM dba, by forma udzielenia zgody uwzględniała te wymogi.

**Czy można wycofać swoją zgodę?**

Co ważne, należy również poinformować pacjenta, że może łatwo i skutecznie wycofać udzieloną zgodę. W praktyce oznacza to, że jeśli zgoda była pozyskana na przykład
za pośrednictwem strony internetowej, jej odwołanie powinno być możliwe za pomocą tej samej strony. Odwołanie zgody oznacza, że nie można tych danych dłużej przetwarzać w celu, w jakim zostały zebrane, nie wpływa to jednak na legalność operacji przetwarzania sprzed momentu wycofania zgody.

|  |
| --- |
| ***Podstawy prawne RODO:******Artykuł 6 Zgodność przetwarzania z prawem****1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:**a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;**b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;**c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;**d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;**e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;**f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, kiedy 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 myśl art. 6, 7 i 9 RODO****Artykuł 7 Warunki wyrażenia zgody****1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.**2. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.**3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.**4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.****Artykuł 9 Przetwarzanie szczególnych kategorii danych osobowych****1. 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.**2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:**a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;**b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującym odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;**c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;**d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;**e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;**f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;**g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;**h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;**i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;**j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.**3. Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.**4. Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.* |

1. **DANE OSOBOWE W MPM**

## **Jakie dane osobowe przetwarza MPM?**

Mała Placówka Medyczna przetwarza przede wszystkim dane osobowe niezbędne
do realizacji celów, jakimi są profilaktyka zdrowotna, medycyna pracy, rejestracja
i świadczenie usług opieki zdrowotnej oraz ochrona żywotnych interesów[[6]](#footnote-6) osoby, której dane dotyczą. W określonych wypadkach MPM przetwarza także dane osobowe
w związku z działaniami marketingowymi oraz realizacją badań klinicznych
i naukowych.

Przepisy sektorowe wskazują jednoznacznie zakres danych zbieranych przez MPM
w deklaracji wyboru oraz w systemie informacji w ochronie zdrowia. Ponadto przepisy określają minimalny zakres informacji jakie powinny znaleźć się w dokumentacji medycznej.

W trosce o prawa osoby fizycznej członkowie kodeksu przyjmują, że w ramach udzielania świadczeń zdrowotnych będą zbierać wyłącznie dane osobowe niezbędne do realizacji celów nałożonych na MPM przez przepisy obowiązującego prawa.

## **Jaki zakres danych może przetwarzać MPM dla celów medycznych?**

Na potrzeby kodeksu przyjmuje się, że będą to dane wymienione w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta, ustawie o systemie informacji w ochronie zdrowia oraz ustawie o podstawowej opiece zdrowotnej, które zostały przedstawione
w poniższym wykazie.

|  |  |
| --- | --- |
| Zakres danych | Podstawa prawna |
| Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta(w art. 25 ustawodawca określił jedynie minimalną zawartość dokumentacji medycznej) | Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (art. 4 Ustawy wskazuje jednoznacznie, że w systemie informacji są przetwarzane dane dotyczące usługobiorców, które obejmują:) | Ustawa z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (w art. 10 ustawodawca wskazuje na zamknięty katalog danych zbieranych w Deklaracji wyboru:) |
| Imię i nazwisko | + | + | + |
| Nazwisko rodowe |  | + | + |
| Płeć | + | + | + |
| Obywatelstwo |  | + |  |
| Wykształcenie |  | + |  |
| Numer pesel | + | + | + |
| Data urodzenia | + | + | + |

|  |  |  |  |
| --- | --- | --- | --- |
| Ew. numer paszportu albo innego dokumentu stwierdzającego tożsamość | + | + | + |
| Adres miejsca zamieszkania | + | + | + |
| Adres do korespondencji |  | + |  |
| Adres miejsca pobytu na terytorium Rzeczypospolitej, jeżeli dana osoba nie ma na terytorium Rzeczypospolitej Polskiej miejsca zamieszkania |  | + |  |
| Adres poczty elektronicznej |  | + | + |
| Numer i rodzaj dokumentu potwierdzającego prawo do świadczeń opieki zdrowotnej finansowanych ze środków publicznych |  | + |  |
| Stopień niepełnosprawności |  | + |  |
| Rodzaj uprawnień oraz numer i termin ważności dokumentów potwierdzających uprawnienia do świadczeń opieki zdrowotnej określonego rodzaju oraz datę utraty tych uprawnień |  | + |  |
| Numery identyfikacyjne i numery ewidencyjne nadawane usługobiorcom przez płatników lub usługodawców |  | + |  |
| Datę zgonu |  | + |  |
| Informacje o prawie do świadczeń opieki zdrowotnej finansowanych ze środków publicznych |  | + |  |
| Numer identyfikujący płatnika |  | + |  |
| Numer telefonu kontaktowego |  | + | + |
| Informacje o sprzeciwie zawartym w centralnym rejestrze sprzeciwów na pobranie komórek, tkanek i narządów ze zwłok ludzkich… |  | + |  |
| Jednostkowe dane medyczne |  | + |  |
| Nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania (w przypadku, gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody) |  |  | + |
| Dane identyfikujące osobę upoważnioną\* przez pacjenta do informacji o jego stanie zdrowia | Na podstawie §8 rozporządzenia z dnia 8 grudnia 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania jest to imię i nazwisko oraz dane umożliwiające kontakt z osobą upoważnioną |  |  |
| Dane identyfikujące osobę upoważnioną\* przez pacjenta do uzyskiwania dokumentacji medycznej | Na podstawie §8 rozporządzenia z dnia 8 grudnia 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania jest to imię i nazwisko.  |  |  |
| Informacje o osobie upoważnionej\* przez pacjenta do odbioru recepty lub zlecenia | Art.42 Ustawy o zawodach lekarza i lekarza dentysty wskazuje, że dane o osobie, która odebrała receptę lub zlecenie należy odnotować (dołączyć) w dokumentacji medycznej.  |  |
| Ponadto – |
| do danych, które może przetwarzać MPM, zalicza się także wszelkie dokumenty dostarczone przez pacjenta, które na jego wyraźne życzenie dołączane są do dokumentacji medycznej. |

W celu **minimalizacji** zbieranych danych członkowie kodeksu określają, że dla potrzeb identyfikacji osoby upoważnionej przez pacjenta obowiązkowymi danymi podawanymi podczas składania oświadczenia będą: imię i nazwisko oraz data urodzenia osoby upoważnionej (należy unikać zbierania numerów PESEL).

Podczas wizyty lekarskiej pacjent może podać lekarzowi informacje dotyczące chorób genetycznych, życia seksualnego, informacje o nałogach, może to być także informacja o przynależności wyznaniowej (pacjent może nie wyrazić zgody
na wykonanie proponowanego zabiegu ze względu na swoje wyznanie). Powyższe dane są niezbędne do prawidłowego procesu leczenia pacjenta i mogą być zbierane przez MPM – ich podanie jednak zawsze jest dobrowolne.

1. **ZBIERANIE DANYCH OSOBOWYCH**

**Od kogo MPM otrzymuje dane osobowe?**

|  |  |
| --- | --- |
| **Od kogo MPM otrzymuje dane osobowe** | **W jaki sposób** |
| Pacjent lub jego przedstawiciel ustawowy | Osobiście (np. podczas rejestracji, wizyty lekarskiej), pocztą (np. przesyłając wnioski, zapytania), elektronicznie (np. mailem lub poprzez platformę służącą do rejestracji on-line) |
| Osoba upoważniona przez pacjenta | Osobiście, pocztą, elektronicznie (np. jw.) |
| Kontrahenci (np. laboratorium) | Osobiście, pocztą, elektronicznie (np. za pomocą systemu umożliwiającego dostęp do wyników pacjentów on-line) |

**Jakie procedury należy opracować na potrzeby zbierania danych?**

Niezależnie od sposobu zbierania danych osobowych, MPM musi w razie konieczności wykazać, że **dane osobowe zostały pozyskane zgodnie z prawem**. W związku z tym opracowuje odpowiednie procedury dotyczące zbierania danych osobowych, instrukcje dotyczące przyjmowania oraz sprawdzania dokumentów, które wpływają do placówki (niezależnie od tego czy jest to forma papierowa czy elektroniczna) oraz identyfikacji osób, których dotyczą dane.

Na każdym etapie przetwarzania danych osobowych bardzo ważna jest weryfikacja zarówno osoby, której dane przetwarzamy, jak i osoby, której udostępniamy dane osobowe. W związku z powyższym ADO MPM wyraźnie informuje personel odpowiedzialny za przetwarzanie danych osobowych, pacjentów oraz osoby trzecie, które chcą uzyskać dostęp do danych, o tym jakie dokumenty mogą być wymagane przez MPM w celu weryfikacji tożsamości. Taką informację zamieszcza w widocznym miejscu w strefach, gdzie zbiera się dane osobowe (np. rejestracja, tablica przed gabinetem lekarskim)

**Pacjent może dostarczyć deklarację wyboru świadczeniodawcy do MPM
na piśmie lub za pomocą SIM.** Każda wspomniana forma wymaga podpisu pacjenta. W wypadku dokumentacji elektronicznej wymagany jest podpis kwalifikowany albo potwierdzony profilem zaufanym ePUAP. Obowiązkiem MPM jest sprawdzenie czy ww. deklaracja została wypełniona prawidłowo i czy zawiera wyłącznie dane wskazane w ustawie o podstawowej opiece zdrowotnej**.**

**Dokumenty wymagane do weryfikacji tożsamości pacjenta lub osoby chcącej uzyskać dostęp do danych osobowych:**

1. dowód osobisty lub inny dokument ze zdjęciem potwierdzający tożsamość (np. paszport)
2. akt urodzenia dziecka oraz dokument potwierdzający tożsamość
(jeżeli personel medyczny ma wątpliwości czy osoba zgłaszająca się na wizytę z dzieckiem lub wnioskująca o informację/dokumentację medyczną dotyczącą małoletniego pacjenta jest jego rodzicem i tym samym ma prawo wglądu do danych osobowych)
3. odpis orzeczenia sądowego, np. ustanawiającego opiekę nad niepełnosprawnym lub małoletnim oraz dokument potwierdzający tożsamość.

**W przypadku wszystkich powyższych dokumentów, MPM nie kopiuje ich ani nie skanuje do dokumentacji, prosi jedynie o ich okazanie.**

**Jak długo MPM może przechowywać dane osobowe?**

Dane osobowe powinny być przechowywane nie dłużej, niż o niezbędne do realizacji celów, dla których dane te zostały zebrane (art. 5 ust. 1 pkt e RODO). Okres przechowywania jest zatem uzależniony od celu przetwarzania. Jeśli więc MPM zbiera dane w celu:

– zapewnienia opieki medycznej, dane można przechowywać 20 lat (termin liczony
od końca roku kalendarzowego, kiedy dokonano ostatniego wpisu w dokumentacji)
lub nawet 30 lat w wypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia – stosownie do przepisów ustawy o prawach pacjenta i Rzecznika Praw Pacjenta lub innych przepisów (między innymi w przepisach regulujących medycynę pracy);

– przesyłania pacjentom materiałów marketingowych, to dane te można przetwarzać przez okres, kiedy MPM posiada ważną zgodę pacjenta (np. do czasu jej wycofania), a po odwołaniu tej zgody – przez okres 10 lat, po którym przedawniają się roszczenia związane z działalnością marketingową MPM;

- dochodzenia lub obrony roszczeń związanych z udzielanymi świadczeniami, to dane przetwarza się przez okres przedawnienia się tych roszczeń określony w przepisach kodeksu cywilnego.

|  |  |  |
| --- | --- | --- |
| **Rodzaj dokumentacji medycznej** | **Okres przechowywania (w latach)** | **Sposób liczenia terminu** |
| Dokumentacja medyczna w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia | 30 lat | Termin liczony od końca roku kalendarzowego, kiedy nastąpił zgon |
| Dokumentacja medyczna zawierająca dane niezbędne do monitorowania losów krwi i jej składników | 30 lat | Termin liczony od końca roku kalendarzowego, kiedy dokonano ostatniego wpisu w dokumentacji |
| Zdjęcia rentgenowskie przechowywane poza dokumentacją medyczną pacjenta | 10 lat | Termin liczony od końca roku kalendarzowego, kiedy wykonano zdjęcie |
| Skierowania na badania i zlecenia lekarza | 5 lat | Termin liczony od końca roku kalendarzowego, kiedy udzielono świadczenia będącego przedmiotem skierowania lub zlecenia |
| Skierowania na badania i zlecenia lekarza - w wypadku, gdy świadczenie zdrowotne nie zostało udzielone z powodu niezgłoszenia się pacjenta w ustalonym terminie, chyba że pacjent odebrał skierowanie | 2 lata | Termin liczony od końca roku kalendarzowego, kiedy wystawiono skierowanie |
| Dokumentacja medyczna dotycząca dzieci do ukończenia 2. roku życia | 22 lata | Termin liczony od końca roku kalendarzowego, kiedy dokonano ostatniego wpisu w dokumentacji |
| Pozostała dokumentacja medyczna | 20 lat | Termin liczony od końca roku kalendarzowego, kiedy dokonano ostatniego wpisu w dokumentacji |

1. **FORMY PRZETWARZANIA DANYCH**

**W jakiej formie MPM przetwarza dane osobowe?**

MPM przetwarza dane osobowe pacjentów w formie papierowej, elektronicznej, papierowej i elektronicznej. Każda z tych form wymaga odpowiedniej ochrony
i dostosowania zabezpieczeń.

MPM musi zapewnić integralność danych i stały dostęp do dokumentacji osobom upoważnionym. W wypadku dokumentacji medycznej każdy wpis w niej dokonywany – niezależnie od formy jej prowadzenia – musi być opatrzony podpisem osoby
go wprowadzającej a każda zmiana musi być zarejestrowana.

W wypadku dołączania do dokumentacji prowadzonej w formie elektronicznej dokumentów utworzonych w postaci papierowej należy stworzyć procedurę, która krok po kroku opisuje, w jaki sposób z zachowaniem wiarygodności danych powinny one być wprowadzane. Należy także opisać, co zrobić z oryginałem dokumentu, utworzonym
w wersji papierowej po wprowadzeniu go do systemu informatycznego, uwzględniając przy tym ust. 2 §81 Rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania, który wyraźnie wskazuje, że dołączenie do dokumentacji elektronicznej dokumentów utworzonych w innej postaci powinno być dokonane przez osobę upoważnioną przez MPM w sposób zapewniający czytelność, dostęp i spójność dokumentacji. Po wykonaniu digitalizacji danych oryginał powinien być wydany pacjentowi lub trwale zniszczony, w sposób uniemożliwiający identyfikację pacjenta. Zdigitalizowany dokument nadal jest natomiast ważnym nośnikiem informacji w rozumieniu kodeksu cywilnego, nie ma potrzeby zatem przetrzymywania papierowej wersji dokumentu.

**Jakie obowiązki spoczywają na MPM w odniesieniu do dokumentacji medycznej?**

MPM jest zobowiązana do **prowadzenia**, **przechowywania** i **udostępniania** dokumentacji medycznej zgodnie z obowiązującymi przepisami prawa. Jednocześnie musi zapewnić **ochronę wszelkich danych** zawartych w tej dokumentacji, niezależnie od formy jej prowadzenia (papierowej lub elektronicznej).

W tym celu MPM zapewnia, że w dokumentacji medycznej są przechowywane wyłącznie dane niezbędne do udzielania świadczeń zdrowotnych (np. informacje zbierane podczas rozmowy/wywiadu istotne dla lekarza czy pielęgniarki w procesie leczenia) oraz dane dostarczone przez pacjenta.

W wypadku dołączania do dokumentacji medycznej dokumentów dostarczanych przez pacjenta (np. wyników badań wykonanych bez zlecenia lekarza), należy
go poinformować o tym, że dokument włączony do dokumentacji medycznej nie może być z niej usunięty.

Ponadto MPM musi zadbać o to, żeby zapisy sporządzane w dokumentacji medycznej (zarówno papierowej jak i elektronicznej) były dokonywane wyłącznie przez osoby
do tego upoważnione. Dokumentacja medyczna musi być prowadzona w sposób, który gwarantuje jej **prawidłowość**, **integralność** i **poufność**. To znaczy, że musi być
ona prowadzona w sposób czytelny i zapewniający osobom upoważnionym dostęp
do jej elementów bez zbędnej zwłoki[[7]](#footnote-7).

Mała Placówka Medyczna musi zapewnić, by dostęp do dokumentacji medycznej miały wyłącznie osoby upoważnione przez administratora, w zakresie niezbędnym
do wykonywania swoich zadań. Na podstawie obowiązujących przepisów[[8]](#footnote-8) mogą to być osoby wykonujące zawód medyczny (np. lekarze/lekarki, pielęgniarki/pielęgniarze),
a także inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych (np. rejestratorki/rejestratorzyinformatycy/osoby odpowiedzialne za IT.

Ponadto MPM jest zobowiązany udostępniać dokumentację medyczną podmiotom upoważnionym, w sposób wskazany przez wnioskodawcę.

**Przykłady zarządzania dokumentacją prowadzoną w formie papierowej
i elektronicznej:**

|  |  |  |
| --- | --- | --- |
| Przykłady | Dokumentacja w formie papierowej | Dokumentacja w formie elektronicznej |
| Dokumentacja medyczna indywidualna i zbiorcza, deklaracje wyboru |
| Dostęp do dokumentacji | Określenie kto i na jakich zasadach może mieć dostęp do dokumentów (upoważnienia dla pracowników) | Nadanie dostępu upoważnionym pracownikom do pracy w systemie informatycznym i określenie zakresu czynności, jakie dane osoba może wykonywać na danych. |
| Przechowywanie  | Przykład – wypełnione deklaracje wyboru przechowuje się w miejscu udzielania świadczeń, dokumenty zawierające dane osobowe przechowuje się w szafach zamykanych na klucz. | Własna infrastruktura informatyczna (serwery, infrastruktura sieciowa, oprogramowanie, odpowiednie pomieszczenie przystosowane do pracy serwera, zapewnienie opieki i serwisu sprzętu i oprogramowania. Outsourcing – na podstawie umowy powierzenia |
| Udostępnianie | Przykład – MPM ma obowiązek zapewnienia dostępności deklaracji wyboru pacjentom, których one dotyczą.Dokumentacja medyczna może być udostępniona w sposób określony w ustawie o prawach pacjenta i Rzeczniku Praw PacjentaMPM tworzy odpowiednie instrukcje dotyczące udostępnienia dokumentacji medycznej w formie papierowej. | MPM udostępnia dokumentację medyczną za pośrednictwem środków komunikacji elektronicznej (e-mail, e-PUAP) oraz na informatycznym nośniku danych (płyta CD, pendrive)MPM tworzy odpowiednie instrukcje dotyczące udostępnienia dokumentacji medycznej w formie elektronicznej. |
| Powierzenie | ADO może powierzyć przetwarzanie danych osobowych wyłącznie na podstawie umowy zawartej z procesorem. | ADO może powierzyć przetwarzanie danych osobowych wyłącznie na podstawie umowy zawartej z procesorem. |
| Archiwizowanie | ADO określa okresy przechowywania dokumentacji papierowej (uwzględniając przy tym ustawowo określone okresy przechowywania dokumentacji medycznej, o których mowa powyżej w pkt. „Jak długo MPM przetwarza dane osobowe?”) oraz odpowiednie warunki jej przechowywania. Jeżeli ADO nie może zapewnić właściwego zabezpieczenia archiwalnej dokumentacji może na podstawie umowy powierzyć przechowywanie takich danych osobowych podmiotowi zewnętrznemu. | ADO określa okresy przechowywania danych w wersji elektronicznej (uwzględniając przy tym ustawowo określone okresy przechowywania dokumentacji medycznej, o których mowa powyżej w pkt. „Jak długo MPM przetwarza dane osobowe?”) oraz sposoby jej archiwizowania i zasady bezpieczeństwa nośników danych. |
| Niszczenie | ADO określa procedury dotyczące niszczenia papierowej dokumentacji w sposób uniemożliwiający jej późniejsze odczytanie, np. przez niszczenie siłami własnymi – za pomocą niszczarki, podpisanie umowy z firmą zewnętrzną zajmującą się profesjonalnym niszczeniem nośników danych. | ADO określa procedury dotyczące niszczenia danych w formie elektronicznej uwzględniające trwałe usunięcie danych lub trwałe zniszczenie nośników danych. |

1. **ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH**

Zarządzając przetwarzaniem danych osobowych MPM powinien regularnie kontrolować i doskonalić funkcjonujący w przedsiębiorstwie system ochrony danych osobowych, który można podzielić na trzy podstawowe elementy:

1. bezpieczeństwo,
2. dokumentacja,
3. zasoby ludzkie.

**W jaki sposób MPM powinien zarządzać bezpieczeństwem danych osobowych?**

W celu sprawowania kontroli nad danymi osobowymi przetwarzanymi w MPM należy wprowadzić procedury umożliwiające monitorowanie wszelkich czynności wykonywanych na danych.

Kontrola przetwarzania danych osobowych w MPM polega przede wszystkim na:

a) inwentaryzacji zasobów – MPM ustala jakie dane osobowe i w jaki sposób przetwarza, np. dane osobowe pacjentów zbierane w deklaracjach wyboru, dane utrwalane w dokumentacji medycznej – w wersji papierowej i elektronicznej. Dane przechowywane w szafach kartotecznych, zamykanych na klucz; na serwerze,
w chmurze, na zewnętrznych nośnikach danych;

b) określeniu jakie obowiązki, w związku z przetwarzaniem powyższych danych nakłada na administratora danych osobowych RODO;

c) analizie ryzyka;

d) prowadzeniu audytów ochrony danych osobowych podczas, których sprawdzany jest niezbędny zakres zbieranych informacji, adekwatność i stosowanie procedur, środki ochrony technicznej;

e) przeglądzie upoważnień i uprawnień dostępu do danych osobowych.

**MPM musi pamiętać o cyklicznym przeprowadzaniu analizy ryzyka, audytów bezpieczeństwa oraz przeglądów upoważnień i uprawnień**.

Organizując zarządzanie bezpieczeństwem danych osobowych MPM powinien określić, jakie dane osobowe są niezbędne do realizacji konkretnego celu (np. dane osobowe pacjentów podawane w deklaracji wyboru, dane osobowe zbierane w celu udzielenia świadczenia zdrowotnego) oraz w jakiej formie je przetwarza (papierowo/elektronicznie). MPM określa również kto i na jakich zasadach musi mieć dostęp do tych danych (lekarze, pielęgniarki, rejestratorski, pracownicy statystyki medycznej).

**Jak należy przeprowadzić szacowanie ryzyka?**

MPM cyklicznie przeprowadza **analizę ryzyka** oraz jeżeli wynika to z analizy **ocenę skutków. Analizując ryzyko MPM** identyfikuje zagrożenia związane z przetwarzaniem danych osobowych oraz określa ich wartość.

Ryzyko wzrasta, gdy:

- przetwarzane są dane osobowe o stanie zdrowia,

- dane przechowywane są w sposób dostępny dla osób nieupoważnionych (np. wyniki badań leżące na kontuarze otwartej recepcji),

- dokumentacja medyczna przechowywana jest w sposób narażający ją na zniszczenie (np. w piwnicy pod rurami kanalizacyjnymi).

Ryzyko maleje gdy:

- przetwarzane są dane osobowe zwykłe,

- dokumentacja przechowywana jest w zamkniętych szafach kartotecznych,

- archiwum z dokumentacją medyczną zapewnia odpowiednie warunki jej przechowywania (temperatura, wilgoć, kontrola dostępu pracowników MPM).

MPM musi ocenić jakie jest ryzyko naruszenia praw i wolności osób, których dane przetwarza oraz jakie ryzyko dla placówki niesie za sobą przetwarzania tych danych.

O tym, czym jest jest ryzyko dla praw i wolności mówi motyw 85 RODO: *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.*

Żeby to zrobić, powinien przeprowadzić szczegółową analizę czynności przetwarzania prowadzonych w placówce (np. rejestracja pacjentów) i na tej podstawie ocenić ryzyko, na jakie mogą być narażone dane osobowe. MPM musi określić, jakie są możliwe rodzaje ryzyka utraty, zniszczenia, nieuprawnionego udostępnienia danych osobowych, jakie skutki dane ryzyko niesie dla osoby fizycznej, której dane dotyczą. Ponadto MPM musi określić prawdopodobieństwo wystąpienia poszczególnych rodzajów ryzyka i określić sposób postępowania w celu ich eliminacji lub minimalizacji.

Każdy proces (czynność przetwarzania danych) zachodzący w MPM należy podzielić
na trzy obszary:

- **ludzie**, którzy przetwarzają dane osobowe;

- **środowisko informatyczne**, gdzie przetwarza się dane osobowe oraz fizyczne nośniki danych (jak komputery, dyski zewnętrzne);

- **przepływ danych** osobowych w danym procesie.

Zdefiniowanie osób biorących udział w danym procesie jest niezwykle ważne z punktu widzenia ochrony danych osobowych oraz ryzyka związanego z ich przetwarzaniem. Chodzi oczywiście o wskazanie stanowisk służbowych biorących udział w procesie,
a nie wskazywania osób z imienia i nazwiska. Precyzyjne określenie środowisk informatycznych oraz fizycznych nośników danych wykorzystywanych w procesie pozwala z kolei ocenić ryzyko z punktu widzenia zabezpieczeń, jakie stosuje MPM
by chronić należycie dane osobowe. Kluczową rzeczą w procesie oceny ryzyka jest natomiast dokładny opis przepływu danych osobowych w danym procesie. Chodzi o to, aby MPM miał pełną jasność co do tego, kto, kiedy i w jakim celu przetwarza dane osobowe oraz jaką drogą wszedł w ich posiadanie. Analizujemy w tym kroku po kolei: jakie dane przetwarzamy (mapowanie), niezbędność i proporcjonalność przetwarzania (podstawy prawne) oraz procedury (np. sposób realizowania praw pacjentów).

Po takiej analizie MPM musi określić jakie są możliwe zagrożenia związane
z przetwarzaniem danych osobowych w poszczególnych procesach, które mogą oznaczać ryzyko **utraty, zniszczenia i nieuprawnionego udostępnienia** danych osobowych. Dla każdego z tych zagrożeń należy ocenić **prawdopodobieństwo** jego wystąpienia oraz ocenić, jakie **konsekwencje** dla praw i wolności osób może mieć naruszenie ochrony danych osobowych. Po ocenie prawdopodobieństwa zdarzenia
oraz możliwych konsekwencji dla osoby, której dane dotyczą, należy ocenić ryzyko
w skali: duże ryzyko dla praw i wolności pacjenta (np. uniemożliwienie dalszego właściwego leczenia z powodu utraty dostępności do bazy danych – MPM może wtedy nie móc określić jakie leki i w jakiej ilości należy podać pacjentowi, co zagraża jego zdrowiu i życiu), średnie ryzyko dla praw i wolności pacjenta (przekazanie wyników badania krwi niewłaściemu pacjentowi) lub małe ryzyko dla praw i wolności pacjenta (zgubienie zaszyfrowanego pendrive`a z wynikami badań).

Ocena ryzyka dla praw i wolności osób, których dane dotyczą jest więc wypadkową dwóch czynników. Są nimi prawdopodobieństwo wystąpienia zagrożenia (kradzież dokumentów, pożar w budynku, wyciek danych w postaci przekazania wyników badań niewłaściwemu pacjentowi) oraz możliwych konsekwencji dla osoby, której te dane dotyczą. Tymi konsekwencjami mogą być np. wykonanie niewłaściwych świadczeń medycznych, utrata dobrej opinii w lokalnej społeczności, wyższa składka ubezpieczeniowa, plotkowanie na temat danej osoby. Jest to, co naturalne, proces ciągły
i wymagający poprawy w zakresie mechanizmów kontrolnych w kontekście nowo odkrytych zagrożeń, których wcześniej nie zidentyfikowaliśmy.

Po przeprowadzeniu tej analizy, koniecznym jest zastosowanie mechanizmów kontrolnych. Mechanizmy kontrolne stanowią środki techniczne i organizacyjne, o których mowa w RODO. Stosownie do procesu należy stosować adekwatne mechanizmy kontrolne. I tak :

– w odniesieniu do osób mechanizmem kontrolnym może być nadanie upoważnień do dostępu do danych. Rolę środka organizacyjnego będzie też pełnił regulamin wewnętrzny dotyczący zasad zachowywania się w budynku podmiotu leczniczego oraz podział zadań służbowych.

– w odniesieniu do środowiska informatycznego oraz fizycznych nośników danych należy określić takie mechanizmy kontrolne jak: logiczne zabezpieczenia systemów np. hasła do dysków, systemów, pendrivów, poszczególnych plików
z danymi osobowymi pacjentów, oprogramowanie antywirusowe, zapory sieciowe itp. oraz zabezpieczenia fizyczne np. kłódki do szafek, szyfry do sejfów, klucze
do pomieszczeń i szafek, karty dostępu, systemy alarmowe, gaśnice, żaluzje antywłamaniowe.

– w odniesieniu do przepływu danych należy ocenić czy w danym procesie
nie występuje zbyt duża liczba osób bądź czy dane osobowe nie są bez potrzeby przekazywane wewnątrz MPM. Każdorazowo należy wyznaczyć najniższą
z możliwych liczbę osób uczestniczących w danym procesie przy jednoczesnej minimalizacji przetwarzanych danych osobowych

**Przykład 2: Przykłady zagrożeń i zabezpieczeń**

Żeby właściwie chronić dane osobowe, należy ustalić na jakie zagrożenia mogą być narażone dane osobowe pacjentów przetwarzane w MPM.

|  |  |  |
| --- | --- | --- |
| Ochrona przed | Przykłady zagrożeń w zależności od formy przetwarzania danych | Zabezpieczenie |
| Dane osobowe w formie papierowej | Dane osobowe w formie elektronicznej | organizacyjne | techniczne |
| Zniszczeniem | zalanie | Wirus | Zabezpieczenie systemu informatycznego poprzez zainstalowanie antywirusa oraz tworzenie kopii zapasowych.Stworzenie instrukcji dotyczącej postępowania w przypadku zagrożenia | Fizyczne zabezpieczenie dokumentacji papierowej poprzez umieszczenie jej w metalowych szafach kartotecznych z dala od rur wodociągowych, umieszczenie dokumentacji na podwyższeniu – nie bezpośrednio na podłodze. |
| Utratą | Pożar, kradzież | Kradzież nośnika danych, atak hackerski | Kontrola dostępu pracowników | Zamki, alarmy, drzwi antywłamaniowe, rolety, firewalle, antywirusy, back-upy |
| Udostępnieniem osobie nieupoważnionej | Pomyłka przy wydawaniu dokumentacji medycznej | Przesłanie danych na niewłaściwy adres e-mail | Zasady udostępniania dokumentacji medycznej | Odpowiednie poziomy dostępu w systemach IT dla pracowników MPM |
| Nieuprawnioną modyfikacją | Fałszowanie zapisów w dokumentacji medycznej | Wprowadzanie zatwierdzonych zmian w dokumentacji elektronicznej bez odnotowania w systemie danej operacji | Zasady postępowania dokumentacji medycznej | Odpowiednie poziomy dostępu w systemach IT dla pracowników MPM |
| Nieuprawnionym dostępem | Dostęp do dokumentacji medycznej personelu sprzątającego | Dostęp do wszelkich zapisów prowadzonych w elektronicznej dokumentacji medycznej rejestratorek medycznych | Zasada czystego biurka, szafki zamykane na klusze, nadzór nad osobami sprzątającymi | Wylogowywanie się z systemów i aplikacji, stosowanie wygaszaczy ekranów, folie prywatyzujące |

Jeżeli przeprowadzona przez MPM analiza ryzyka (podczas której uwzględniono charakter, zakres, kontekst i cel przetwarzania) wykaże, że dany rodzaj przetwarzania
z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, konieczne będzie dokonanie oceny skutków dla ochrony danych osobowych. Jest to proces bardzo podobny do szacowania ryzyka, musi jednak uwzględniać również propozycje, jakie środki organizacyjne i techniczne należy wdrożyć, aby poziom ryzyka dla danego procesu obniżyć z poziomu wysokiego
do średniego lub małego[[9]](#footnote-9). Jeśli MPM nie będzie jednak w stanie zminimalizować ryzyka, konieczna będzie konsultacja z Prezesem Urzędu Ochrony Danych Osobowych[[10]](#footnote-10).

|  |
| --- |
| ***Podstawy prawne RODO:******Artykuł 24 Obowiązki administratora****1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.**2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.**3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.****Artykuł 35 Ocena skutków dla ochrony danych****1. 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.**2. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.**3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, 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, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10; lub**c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.**4. Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust. 1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych, o której mowa w art. 68.**5. Organ nadzorczy może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych.**6. Jeżeli wykazy, o których mowa w ust. 4 i 5, obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63.**7. Ocena 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, o którym mowa w ust. 1; oraz**d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.**8. Oceniając - w szczególności do celów oceny skutków dla ochrony danych - skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 40.**9. W stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.**10. Ust. 1-7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej - chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.**11. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.* |

**Jakie środki techniczne i organizacyjne (mechanizmy kontrolne) MPM powinien wdrożyć?**

Po przeprowadzeniu analizy administrator będzie mógł zadecydować o technicznych
i organizacyjnych zabezpieczeniach, takich jak:

- **zabezpieczenia techniczne:** instalacja przeciwpożarowa, instalacja alarmowa, zabezpieczenie okien, drzwi zamykane na klucz, szafki zamykane na klucz, odpowiednie ustawienie monitorów ekranowych;

- **zabezpieczenia organizacyjne**: procedury, instrukcje (dot. nadawania upoważnień
i uprawnień, korzystania z poczty elektronicznej, udostępniania dokumentacji medycznej, polityka kluczy, rejestrowanie pacjenta, archiwizowanie, niszczenie dokumentacji).

**Dostosowanie zabezpieczeń technicznych**

Po przeprowadzeniu analizy ryzyka administrator dobiera odpowiednie do zagrożeń zabezpieczenia budynku oraz pomieszczeń, gdzie przechowuje się dane osobowe.

Zabezpieczenie dokumentów przechowywanych w formie papierowej oraz elektronicznej – szczególny nacisk należy położyć na dostęp do pomieszczeń, gdzie znajdują się dane osobowe. Należy zabezpieczyć wejścia do pomieszczeń np. poprzez montaż gałko-klamek, każdorazowe zamykanie drzwi na klucz, odpowiednie przechowywanie kluczy do budynku i pomieszczeń.

Bezpieczeństwo informatyczne – należy zadbać, by do przetwarzania danych osobowych używany był odpowiedni sprzęt, programy. Trzeba też wdrożyć odpowiednie procedury informatyczne haseł (np. wymuszanie na użytkownikach żeby hasło miało określoną długość oraz regularnej zmiany haseł), korzystania z poczty elektronicznej (np. zasad ograniczonego zaufania w odniesieniu do korespondencji i załączników od nieznanych nadawców), użytkowania sprzętu informatycznego (np. zasady bezpieczeństwa używania komputerów przenośnych) oraz aplikacji służących do przetwarzania danych osobowych.

W wyniku analizy, na jakie zagrożenia mogą być narażone dane osobowe przetwarzane w MPM, należy dobrać środki zabezpieczające adekwatne do poziomu ryzyka naruszenia ochrony danych osobowych.

Przykład – dane osobowe w MPM przetwarza się zarówno w formie papierowej jak i elektronicznej. Podczas analizy ryzyka stwierdzono, że największym zagrożeniem dla danych osobowych pacjentów może być kradzież dokumentacji papierowej oraz komputera, który pełni funkcję serwera. W związku z powyższym zdecydowano o wprowadzeniu następujących zabezpieczeń technicznych:

* rolety antywłamaniowe, alarm połączony z monitoringiem firmy ochroniarskiej;
* instalacja gaśnic, w tym specjalnej do gaszenia sprzętu elektronicznego;
* osobne przechowywanie komputera, który pełni rolę serwera
i ograniczenie dostępu do pomieszczenia, w którym się znajduje;
* montaż gałko-klamek w drzwiach do gabinetów;
* przechowywanie kluczy do szafek i pomieszczeń w szyfrowanym kluczniku oraz wdrożenie zabezpieczeń organizacyjnych;
* nadawanie upoważnień wszystkim osobom zatrudnionym w MPM, które mają dostęp do danych osobowych;
* szkolenie personelu;
* ograniczona liczba osób znająca kod aktywujący i wyłączający alarm;
* ograniczona liczba osób znająca kod do klucznika;
* prowadzenie dokumentacji określającej zasady ochrony danych osobowych (udostępnianie dokumentacji medycznej, korzystanie z poczty elektronicznej, niszczenie dokumentacji).

W wypadku wprowadzania nowego systemu informatycznego/aplikacji, już **na etapie projektowania** takiego rozwiązania, administrator musi **uwzględnić ochronę danych osobowych,** czyli ustalić jakie środki techniczne i organizacyjne będzie musiał zapewnić w celu ochrony tych danych.

**Przykład 1: Ochrona danych osobowych w fazie projektowania:**

Podczas projektowania systemu internetowej rejestracji pacjentów, należy pamiętać o dostosowaniu odpowiednich zabezpieczeń technicznych
i organizacyjnych, tak żeby już na etapie planowania prac związanych z wdrożeniem nowego systemu, uwzględnione zostały koszt wdrożenia, zakres niezbędnych danych, cele przetwarzania oraz ryzyko naruszenia praw i wolności osoby fizycznej.

Jeszcze przed rozpoczęciem wdrożenia nowego systemu, należy wziąć pod uwagę, czy działanie będzie zgodne z przepisami prawa i należy uwzględnić środki niezbędne do zapewnienia tego bezpieczeństwa.

**Przykład 2: Domyślna ochrona danych osobowych:**

System internetowej rejestracji pacjenta, wprowadzany w placówce, może domyślnie przetwarzać tylko te dane, które są niezbędne do osiągnięcia konkretnego celu.

**Przykład 3**: Administrator decydując się na dołączenie do zewnętrznej platformy pozwalającej na rejestrowanie pacjentów, powinien zadbać o podpisanie odpowiedniej umowy z właścicielami systemu, gdzie zamieszczone zostaną zapisy dotyczące, np. **pseudonimizacji** danych wprowadzanych podczas rejestracji,
żeby dostęp do danych był możliwy wyłącznie dla pacjenta oraz osób upoważnionych w MPM.

|  |
| --- |
| ***Podstawy prawne RODO:******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 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.**2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.**3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.****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, 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.**2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.**3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.**4. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratoralub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.* |

**Jaką dokumentację dotyczącą ochrony danych osobowych powinien prowadzić MPM?**

MPM powinien stworzyć **odpowiednią dokumentację** ochrony danych osobowych, która będzie zawierała konkretne instrukcje dotyczące przetwarzania danych osobowych na każdym etapie ich obiegu. Na powyższą dokumentację powinny składać się przede wszystkim **rejestr czynności przetwarzania**, procedury związane
z **naruszeniem ochrony danych osobowych**, które uwzględniają sposób dokumentowania naruszeń i zgłaszania ich do PUODO oraz powiadomienia osoby fizycznej.

Dokumentację dotyczącą ochrony danych osobowych w MPM należy prowadzić
w sposób, który umożliwi administratorowi wykazanie przestrzegania przepisów RODO.

Obowiązkiem MPM, wynikającym z przepisów RODO, jest **prowadzenie rejestru czynności przetwarzania danych osobowych** oraz **dokumentowanie naruszeń ochrony danych osobowych[[11]](#footnote-11)**.

Ponadto MPM zobowiązany jest do wykazania przestrzegania zasad określonych
w rozporządzeniu Unijnym. Żeby to zrobić MPM powinien stworzyć dokumentację odpowiednią do potrzeb ochrony danych osobowych.

Dokumentacja prowadzona przez MPM, w zakresie ochrony danych osobowych, powinna uwzględniać:

- procedury związane z analizą ryzyka i ewentualną koniecznością przeprowadzenia oceny skutków;

- ewidencję naruszeń ochrony danych;

- instrukcje dotyczące: nadawania upoważnień osobom zaangażowanym
w przetwarzanie danych osobowych w placówce; zbierania danych osobowych
(w deklaracjach, dokumentacji medycznej, zbieranych podczas osobistego kontaktu
z pacjentem, od osób trzecich i droga elektroniczną); spełniania obowiązków informacyjnych; powierzenia danych osobowych (jakie warunki ma spełnić podmiot,
z którym MPM podpisuje umowę powierzenia danych osobowych); udostępnienia danych osobowych (zasady udostępniania); niszczenia danych osobowych, zgłaszania naruszeń UODO i informowania osób fizycznych o naruszeniach; sposobu spełnienia obowiązku informacyjnego.

|  |
| --- |
| ***Podstawy prawne RODO:******Artykuł 30 Rejestrowanie czynności przetwarzania****1. Każdy administrator oraz - gdy ma to zastosowanie - przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie 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, 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.**2. 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, dokumentacja odpowiednich zabezpieczeń;**d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.**3. Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym formę elektroniczną.**4. Administrator lub podmiot przetwarzający oraz - gdy ma to zastosowanie - przedstawiciel administratora lub podmiotu przetwarzającego udostępniają rejestr na żądanie organu nadzorczego.**5. Obowiązki, o których mowa w ust. 1 i 2, nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego 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 czynów zabronionych, o czym mowa w art. 10.* |

**W jaki sposób MPM powinien zarządzać zasobami ludzkimi w procesie przetwarzania danych osobowych?**

**MPM powinien upoważnić i przeszkolić** personel biorący udział w procesie przetwarzania danych osobowych (pisemne upoważnienia dla pracowników, które określają zakres ich dostępu do danych, szkolenia dostosowane do specyfiki danego stanowiska pracy) oraz powołać **Inspektora Ochrony Danych Osobowych**

MPM musi zadbać o to, żeby do przetwarzania danych osobowych miały dostęp wyłącznie osoby upoważnione przez ADO. Na podstawie obowiązujących przepisów mogą to być osoby wykonujące zawód medyczny (np. lekarze, pielęgniarki), jak również inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych
(np. rejestratorki, informatycy).

Upoważnienie musi konkretnie określać kto, do jakich danych i w jakim zakresie będzie miał dostęp. Ponadto do zadań MPM należy zapoznanie upoważnionych osób z zasadami dotyczącymi ochrony danych osobowych oraz regularne podnoszenie świadomości
w tym zakresie osób zatrudnionych w placówce.

**Czy MPM musi powołać inspektora ochrony danych (IOD)?**

Zgodnie z Art. 37 ust. 1 RODO powołanie IOD będzie **obowiązkowe między innymi**w następujących przypadkach:

* przetwarzania dokonują organ lub podmiot publiczny,
* główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych.

Pierwsza sytuacja jest w miarę klarowna – wszystkie publiczne MPM muszą wyznaczyć inspektora ochrony danych. Unijne organy ochrony danych zalecają jednak, żeby inspektora powoływały również prywatne jednostki realizujące zadania w interesie publicznym. Takie stanowisko można interpretować jako zachętę do wyznaczenia inspektora przez wszystkie prywatne placówki medyczne udzielające świadczeń opieki zdrowotnej, które są finansowane ze środków publicznych przez Narodowy Fundusz Zdrowia.

Druga okoliczność jest już bardziej ocenna. W tej sytuacji wyznaczenie inspektora ochrony danych będzie konieczne dla administratorów, których główna działalność polega na przetwarzaniu wrażliwych danych osobowych. Jak czytamy w Wytycznych WP 243 Grupy Roboczej Art. 29 (niezależny organ doradczy Komisji Europejskiej
w zakresie ochrony danych osobowych i prywatności), główna działalność oznacza zasadnicze, nie poboczne działanie. Dla przykładu: główną działalnością placówek medycznych będzie udzielanie świadczeń opieki zdrowotnej. „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.

Pojęcie dużej skali przetwarzania jest z kolei jeszcze bardziej nieostre. Zaleca się uwzględnianie następujących czynników przy określaniu, czy przetwarzanie następuje na „dużą skalę”:

* liczba osób, których dane dotyczą – konkretna liczba osób albo procent określonej grupy społeczeństwa, np. kiedy dana placówka medyczna przetwarza dane osobowe niemal wszystkich mieszkańców małej gminy;
* zakres przetwarzanych danych osobowych – ten w przypadku placówek medycznych będzie zawsze szeroki i będzie uwzględniał dane wrażliwe;
* okres, przez jaki dane są przetwarzane – istotną kwestią będzie zgodny
z przepisami, maksymalny czas przechowywania dokumentacji medycznej,
tj. 30 lat;
* zakres geograficzny przetwarzania danych osobowych.

Biorąc pod uwagę powyższe uwarunkowania wydaje się, że MPM powinien wyznaczyć inspektora ochrony danych osobowych. Nie będzie to jednak dotyczyć sytuacji, kiedy przetwarzanie danych pacjentów – klientów, dokonywane będzie przez pojedynczego lekarza.

**Przykład przetwarzania na dużą skalę:** Dane osobowe pacjentów przetwarzane
przez szpital.

**Przykład przetwarzania niemieszczącego się w definicji „dużej skali”:** Dane osobowe pacjentów przetwarzane przez pojedynczego lekarza, w ramach wykonywania działalności leczniczej.

Nowa ustawa o ochronie danych osobowych przesądza również sposób zawiadamiania organu nadzorczego o danych kontaktowych inspektora wskazując, że „zawiadomienia sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP”. W praktyce oznacza to, że jedyną dopuszczalną formą zgłoszenia IOD jest forma elektroniczna.

Inspektorem ochrony danych może być pracownik bądź współpracownik MPM, który zostanie wyznaczony do sprawowania tej funkcji. Nie ma jednak przeszkód, żeby IOD była osoba spoza placówki, zatrudniona na podstawie umowy o świadczenie usług (np. osoba wskazana przez zewnętrzny podmiot specjalizujący się w obsłudze MPM w zakresie ochrony danych osobowych). Jeśli MPM zdecyduje się na wyznaczenie IOD spośród swojego personelu musi pamiętać, żeby nie była to osoba, której dotychczasowe zadania i obowiązki będą powodować konflikt interesów z nowo pełnioną funkcją (np. kiedy IOD miałaby stać się osoba odpowiedzialna za IT
w placówce, która z jednej strony decydowałaby o stosowanych zabezpieczeniach,
a z drugiej – jako IOD – oceniałaby je pod kątem zgodności z RODO). Ponadto IOD powinien podlegać jedynie kierownictwu MPM.

Osoba pełniąca funkcję IOD powinna cechować się odpowiednią wiedzą
i umiejętnościami – najlepiej, by miała wiedzę nie tylko z zakresu ochrony danych osobowych, ale przede wszystkim z obszaru przepisów sektorowych, regulujących funkcjonowanie MPM.

Wśród wielu zadań IOD, RODO wylicza m.in. monitorowanie przestrzegania RODO
w MPM, współpracę z PUODO oraz pełnienie funkcji punktu kontaktowego
dla pacjentów w sprawach związanych z ochroną danych. Aby należycie realizować te zadania, IODO powinien być angażowany we wszystkie sprawy związane
z działalnością MPM, które mogą mieć wpływ na ochronę danych osobowych pacjentów i pracowników placówki.[[12]](#footnote-12)

|  |
| --- |
| ***Podstawy prawne RODO:******Artykuł 37 Wyznaczenie inspektora ochrony danych****1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, 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, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.**2. Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.**3. Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć - z uwzględnieniem ich struktury organizacyjnej i wielkości - jednego inspektora ochrony danych.**4. W przypadkach innych niż te, o których mowa w ust. 1, administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych. Inspektor ochrony danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające.**5. Inspektor ochrony danych 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.**6. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.**7. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.* |

1. **KOMU I NA JAKICH WARUNKACH MPM MOŻE POWIERZYĆ PRZETWARZANIE DANYCH OSOBOWYCH**

# **Kiedy dochodzi do powierzenia danych osobowych?**

W sytuacji, w której:

* placówka medyczna przekazuje zewnętrznej firmie lub przedsiębiorstwu dane osobowe pacjentów, pracowników, kontrahentów lub innych osób

lub

* placówka medyczna otrzymuje od zewnętrznej firmy lub przedsiębiorstwa dane osobowe pacjentów, pracowników, kontrahentów lub innych osób.

konieczne jest zawarcie **umowy powierzenia przetwarzania danych osobowych**

**Przykłady powierzenia danych osobowych:**

* placówka medyczna -> firma informatyczna
* placówka medyczna -> biuro rachunkowe
* placówka medyczna -> kancelaria prawna
* placówka medyczna -> laboratorium
* placówka medyczna -> placówka medyczna (zlecenie wykonania badań RTG, USG, EKG)
* laboratorium -> placówka medyczna

## **Kiedy MPM jest administratorem, a kiedy podmiotem przetwarzającym?**

**Administrator danych osobowych:**

* ustala cele i sposoby przetwarzania danych osobowych,
* przekazuje dane osobowe na zewnątrz.

**Podmiot przetwarzający (procesor):**

* przetwarza dane osobowe nie na własną rękę, ale w imieniu administratora,
* to jemu przekazywane są dane osobowe

**Przykład:**

Jeżeli placówka medyczna wysyła do laboratorium skierowanie pacjenta na badanie,
dochodzi do powierzenia danych osobowych. **Administratorem** jest placówka medyczna (od niej wyszły dane dotyczące pacjenta), a procesorem – **laboratorium**.

## **Kiedy NIE ZAWIERAMY umowy powierzenia?**

**Przykład 1:**

W sytuacji, w której pacjent sam udaje się do laboratorium na badanie i laboratorium przekazuje wyniki badań bezpośrednio pacjentowi, nie ma podstaw do zawierania umowy powierzenia.

**Przykład 2**

W przypadku świadczenia usług z zakresu medycyny pracy odrębnymi administratorami są:

* pracodawca, który kieruje pracowników na badania medycyny pracy

oraz

* placówka medyczna, która świadczy usługi z zakresu medycyny pracy.

Nie jest to sytuacja współadministrowania w rozumieniu art. 26 RODO, placówki świadczące usługi z zakresu medycyny pracy mają bowiem odrębną podstawę prawną, którą możemy znaleźć w przepisach o służbie medycyny pracy.

Zgodnie z przepisami o służbie medycyny pracy, placówka medyczna:

* musi prowadzić dokumentację medyczną dotyczącą pacjentów

oraz

* nie może udostępniać pracodawcy dokumentacji medycznej jego pracowników.

Powyższe oznacza, że nie istnieje podległość placówki medycznej wobec pracodawcy – oboje są administratorami danych osobowych. **Przy medycynie pracy nie dochodzi
do powierzenia przetwarzania danych osobowych, ale do ich udostępniania**.

Z powierzeniem nie mamy również do czynienia w sytuacji, w której osoba wykonująca zawód medyczny i prowadząca działalność gospodarczą wykonuje swoje zadania
w ramach działalność leczniczej MPM. Jeżeli dana osoba (lekarz czy pielęgniarka):

* nie działa na własny rachunek,
* wykorzystuje bazy danych pacjentów MPM i system informatyczny MPM,
* nie prowadzi też własnej dokumentacji medycznej

to występuje w tej relacji jako osoba upoważniona przez MPM do przetwarzania danych, a nie jej podmiot przetwarzający.

## **Z kim można zawrzeć umowę powierzenia?**

Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą (art. 28 ust. 1 RODO).

## **Co powinna zawierać umowa powierzenia?**

Przepisy dotyczące powierzenia mogą być zawarte:

* w oddzielnej umowie powierzenia,
* w umowie będącej podstawą współpracy stron (placówki medycznej i np. biura księgowego),
* w aneksie do umowy będącej podstawą współpracy stron.

Umowa może mieć formę pisemną, w tym formę elektroniczną.

**Elementy umowy powierzenia:**

1. Przedmiot umowy – *powierzenie danych osobowych pacjentów MPM do firmy
IT w celu administrowania, konserwacji i naprawy systemu informatycznego
w placówce medycznej.*
2. Czas trwania przetwarzania – *czas trwania umowy powierzenia jest równy okresowi trwania umowy z firmą IT.*
3. Charakter przetwarzania – *z wykorzystaniem systemu IT.*
4. Cel przetwarzania – *administrowanie systemem IT na rzecz MPM.*
5. Rodzaj danych osobowych *– dane obecne w systemie IT (imiona, nazwiska, adresy zamieszkania, informacje o stanie zdrowia itp.)*.
6. Kategorie osób, których dane dotyczą – *pacjenci MPM.*
7. Prawa i obowiązki administratora.
8. Obowiązki procesora:
9. zapewnienie, że pracownicy procesora zachowują dane w tajemnicy,
10. zabezpieczenie danych osobowych,
11. korzystanie z usług innego podmiotu przetwarzającego (podpowierzenie)
na warunkach określonych przez administratora zgodnie z RODO,
12. pomoc administratorowi w realizacji praw osób, których dane dotyczą,
13. pomoc administratorowi w realizacji obowiązków wskazanych w art. 32-36 RODO,
14. w zależności od decyzji administratora – usunięcie lub zwrot danych osobowych po zakończeniu współpracy (o ile nic innego nie wynika
z przepisów prawa),
15. udostępnienie administratorowi wszelkich informacji niezbędnych
do wykazania przestrzegania przepisów RODO w zakresie umów powierzenia.

|  |
| --- |
| ***Podstawy prawne RODO:******Artykuł 28 Podmiot przetwarzający****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 ust. 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.* |

1. **POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH**

## **Czym jest naruszenie ochrony danych osobowych?**

**Naruszenie ochrony danych osobowych** to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

* zniszczenia,
* utracenia,
* zmodyfikowania,
* nieuprawnionego ujawnienia,
* nieuprawnionego dostępu do danych

wobec danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez Administratora.

## **Jak dzielimy naruszenia ochrony danych osobowych?**

* naruszenie poufności – niedozwolone lub przypadkowe ujawnienie lub dostęp
do danych osobowych; przykład:
	+ wydanie dokumentacji medycznej osobie nieupoważnionej przez pacjenta,
	+ wyciek bazy danych pacjentów MPM do internetu.
* naruszenie dostępności – niedozwolona lub przypadkowa utrata dostępu
do danych osobowych lub zniszczenie ich; przykład:
	+ zgubienie pendrive’a ze zdjęciami medycznymi pacjenta,
	+ zablokowanie dostępu lekarza do bazy danych pacjentów
	w wyniku ataku *ransmoware* na komputer tego lekarza.
* naruszenie integralności – niedozwolona lub przypadkowa zmiana danych osobowych

## **Jakie zdarzenia są naruszeniem ochrony danych osobowych lub mogą do niego prowadzić?**

O naruszeniu bezpieczeństwa danych osobowych mogą świadczyć w szczególności następujące symptomy:

1. w obrębie pomieszczeń:
2. ślady włamania lub prób włamania do pomieszczeń,
3. ślady włamania lub prób włamania do szuflad, szafek lub szaf, w których przechowywane są dokumenty papierowe lub elektroniczne nośniki informacji, zawierające dane osobowe,
4. w obrębie sprzętu komputerowego:
5. kradzież lub zgubienie komputera lub innego sprzętu komputerowego,
na którym przechowywane są dane osobowe,
6. rozkręcona obudowa komputera,
7. fizyczne zniszczenie komputera lub sprzętu komputerowego (na skutek działania przypadkowego lub celowego, bądź na skutek działania siły wyższej),
8. w obrębie systemu informatycznego:
9. brak możliwości uruchomienia systemu operacyjnego komputera
lub oprogramowania komputerowego,
10. brak możliwości zalogowania się do systemu operacyjnego komputera
lub oprogramowania komputerowego,
11. zmiana zakresu upoważnień użytkownika w systemie informatycznym
(np. brak możliwości wykonywania operacji, których realizacja była wcześniej możliwa lub dostęp do wcześniej zablokowanego programu),
12. inny niż zwykle wygląd systemu operacyjnego lub oprogramowania komputerowego,
13. niestandardowe komunikaty lub komunikaty błędu wyświetlane przez system operacyjny lub oprogramowanie komputerowe,
14. znaczne spowolnienie działania systemu operacyjnego lub oprogramowania komputerowego,
15. zmiana zakresu danych wykorzystywanych w ramach oprogramowania komputerowego,
16. inne:
17. kradzież lub zgubienie dokumentacji papierowej zawierającej dane osobowe,
18. kradzież lub zgubienie elektronicznego nośnika informacji zawierającego dane osobowe.

## **Kto w MPM odpowiada za bezpieczeństwo danych osobowych?**

Każda osoba zatrudniona w placówce medycznej jest odpowiedzialna
za bezpieczeństwo danych osobowych. Pracownik placówki medycznej, który podejrzewa lub stwierdza zdarzenie mogące doprowadzić do naruszenia bezpieczeństwa danych osobowych, zobowiązany jest do natychmiastowego poinformowania o tym **osoby odpowiedzialnej**.

**Osoba odpowiedzialna** to jedna, konkretna osoba, która będzie przyjmowała zgłoszenia o incydentach bezpieczeństwa, udzielała wskazówek dotyczących postępowania oraz dokonywała oceny ewentualnych szkód i wdrażała środki zaradcze.

Taką osobą, w pierwszej kolejności, jest **Inspektor Ochrony Danych** (dawniej Administrator Bezpieczeństwa Informacji). IOD przy realizacji swoich obowiązków
w tym zakresie współpracuje z kierownictwem placówki, informatykiem lub inną osobą, właściwą ze względu na naturę incydentu bezpieczeństwa. W sytuacji, w której IOD
nie został powołany, jego obowiązki w zakresie obsługi incydentów bezpieczeństwa realizuje osoba wyznaczona przez kierownictwo.

## **Jak postępować w razie otrzymania informacji o możliwym naruszeniu ochrony danych?**

W przypadku otrzymania informacji o możliwym naruszeniu ochrony danych IOD,
we współpracy z kierownictwem placówki oraz informatykiem, dokonuje sprawdzenia otrzymanej informacji.

Celem sprawdzenia jest przede wszystkim ustalenie, czy naruszenie ochrony danych skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych. Jeżeli odpowiedź jest twierdząca, MPM:

* zgłasza tę sytuację do PUODO w ciągu 72 godzin od stwierdzenia naruszenia, zgodnie z art. 33 RODO
* niezwłocznie zawiadamia o sytuacji osobę fizyczną, której dotyczy ryzyko, zgodnie z art. 34 RODO. Zawiadomienie jest tworzone jasnym i prostym językiem.

Jeżeli zawiadomienie osób fizycznych, których dotyczy ryzyko, wymaga niewspółmiernie dużego wysiłku, MPM może zrealizować obowiązek zawiadomienia poprzez publiczny komunikat

* na tablicy ogłoszeń w MPM,
* na stronie internetowej MPM,
* przez ogłoszenie w prasie lokalnej.

Oprócz tego MPM zobowiązana jest do prowadzenia rejestru zdarzeń, które mogły stanowić lub stanowią naruszenie ochrony danych osobowych.

**Przykłady:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Zdarzenie** | **Czy zawiadamiać PUODO?** | **Czy zawiadamiać osobę, której dotyczą dane?** | **Uwagi** |
| Administrator przechowywał kopię zapasową archiwum danych osobowych, zaszyfrowaną na płycie CD. Płytę skradziono podczas włamania. | Nie | Nie | Jeżeli dane są zaszyfrowane za pomocą algorytmu zgodnego ze stanem techniki, istnieją kopie zapasowe danych, a unikalny klucz jest bezpieczny, może to być naruszenie niepodlegające obowiązkowi zgłoszenia.Jeżeli jednak w późniejszym czasie coś zagrozi temu bezpieczeństwu, powiadomienie będzie wymagane. |
| Z powodu krótkotrwałej przerwy w dostawie prądu w MPM, pacjenci nie mogli się dodzwonić do rejestracji. | Nie | Nie. | To nie jest naruszenie danych osobowych podlegające obowiązkowi zgłoszenia; niemniej, zdarzenie należy zarejestrować zgodnie z art. 33 ust. 5. RODO. |
| Na administratora przeprowadzono atak za pomocą oprogramowania typu ransomware, w wyniku którego wszystkie dane zostały zaszyfrowane. Nie istnieją kopie zapasowe i nie można odzyskać danych. W toku dochodzenia staje się jasne, że oprogramowanie jedynie szyfruje dane, a w systemie nie wykryto żadnego innego złośliwego oprogramowania. | Tak, ponieważ doszło do utraty dostępności należy powiadomić właściwy organ nadzorczy, jeżeli istnieje możliwość konsekwencji dla osób fizycznych. | Tak, należy powiadomić osoby fizyczne w zależności od charakteru naruszonych danych osobowych i możliwych skutków braku dostępu do danych oraz innych prawdopodobnych konsekwencji. | Jeżeli istniały kopie zapasowe i możliwe jest odzyskanie danych w odpowiednim czasie, o zdarzeniu nie trzeba powiadamiać organu nadzorczego ani osób fizycznych, ponieważ nie doszło do trwalej utraty dostępności lub poufności. Niemniej, w przypadku zgłoszenia do organu nadzorczego, organ może rozważyć przeprowadzenie dochodzenia w celu oceny zgodności z szerszymi wymogami bezpieczeństwa wynikającymi z art. 32. RODO. |
| Z powoducyberataku danemedyczne placówki medycznej są niedostępne przez 30 godzin. | Tak, placówka jest zobowiązana zgłosićnaruszenie, ponieważmoże pojawić sięwysokie ryzykozagrożenia dobrostanui prywatnościpacjentów. | Tak, należy powiadomić osoby fizyczne, których dane naruszono | - |

|  |
| --- |
| ***Podstawy prawne RODO:******Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu****1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.**2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.**3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:**a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;**b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;**c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;**d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.**4. Jeżeli - i w zakresie, w jakim - informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki**5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.****Artykuł 34 Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych****1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.**2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d).**3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:**a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;**b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;**c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.**4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy - biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko - może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.* |

1. **PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ**

**Jakie prawa przysługują pacjentom zgodnie z RODO?**

RODO przyznaje szereg uprawnień wszystkim osobom, których dane są przetwarzane. Dzięki tym uprawnieniom każda z osób będzie w stanie sprawować kontrolę
nad informacjami, które jej dotyczą. Równocześnie nadanie tych uprawnień oznacza dla administratora danych obowiązki. MPM będzie zatem zobowiązany do realizacji następujących praw pacjentów:

* prawo do informacji (obowiązek informacyjny);
* prawo dostępu do danych;
* prawo do sprostowania danych;
* prawo do usunięcia danych (prawo bycia zapomnianym);
* prawo do ograniczenia przetwarzania;
* prawo do przenoszenia danych;
* prawo do sprzeciwu,
* prawo do wycofania zgody w dowolnym momencie.

**Jakie są podstawowe zasady, które MPM powinien stosować realizując uprawnienia osób?**

Realizując prawa pacjentów, MPM dba w szczególności o potwierdzenie tożsamości osoby, która kieruje do MPM określone żądanie. W przypadku wątpliwości, MPM ma prawo poprosić pacjenta o przekazanie informacji potwierdzających jego tożsamość (MPM nie kopiuje ich ani nie skanuje do dokumentacji, prosi jedynie o ich okazanie) , tak by mieć pewność, że realizacja uprawnienia (np. prawa dostępu do danych) nastąpi wobec właściwej osoby i tym samym żadne informacje nie zostaną ujawnione osobom nieupoważnionym. W przypadku braku możliwości potwierdzenia tożsamości,
MPM może nawet odmówić realizacji uprawnienia pacjenta, należy jednak podjąć wszelkie możliwe starania żeby tę tożsamość ustalić (informując przy tym pacjenta jakiego rodzaju informacje musi dostarczyć by potwierdzić jego tożsamość).

MPM dba by wszelkie informacje dotyczące przetwarzania danych osobowych były przekazywane pacjentowi w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Należy więc dbać o to by wszelka komunikacja z pacjentem była prowadzona w sposób dający nie tylko szansę na zapoznanie się
z informacjami, ale przede wszystkim taki, który pozwoli pacjentowi na pełne zrozumienie przekazywanej treści.

MPM powinien również dokumentować wpływające wnioski i prowadzoną w związku
z nimi korespondencję, choćby dla celów dowodowych, w związku z ewentualnymi sporami prowadzonymi z pacjentami.

**W jakiej formie i jak szybko należy odpowiedzieć na żądanie osoby?**

RODO dopuszcza różne formy udzielania informacji – pisemną, elektroniczną
(np. poprzez bezpieczną stronę internetową) i nawet ustną (na żądanie pacjenta,
po uprzednim potwierdzeniu jego tożsamości). Należy jednak pamiętać, że odpowiedzi na żądanie pacjenta należy udzielić niezwłocznie, najpóźniej w terminie miesiąca
od wpłynięcia jego prośby. W tym terminie MPM powinien:

* zrealizować uprawnienie

lub

* poinformować pacjenta o działaniach podjętych w sprawie i konieczności przedłużenia terminu do maksymalnie 3 miesięcy z uwagi na skomplikowany charakter sprawy (MPM musi wskazać przyczyny takie przedłużenia)

lub też

* poinformować o braku możliwości realizacji uprawnienia, wskazując
na przyczyny niepodjęcia działań, prawie pacjenta do złożenia skargi do Urzędu Ochrony Danych oraz skargi do sądu.

MPM może także odmówić realizacji wniosków pacjenta w sytuacji, w której są one nieuzasadnione lub nadmierne, np. kiedy nie udało się zweryfikować tożsamości pacjenta lub kiedy realizacja uprawnienia naruszałaby prawa osób trzecich, lub też mogłaby spowodować ujawnienie tajemnicy lekarskiej. Jeśli zatem odpowiedź na żądanie pacjenta (np. w sytuacji ustawicznego telefonowania z prośbą o udzielenie informacji o danych osobowych w sytuacji wzmożonej pracy personelu MPM w okresie grypowym) wymagałoby zaangażowania personelu medycznego w taki sposób, że inni pacjenci nie mogliby skorzystać ze świadczeń medycznych lub znacznie wydłużyłby się czas realizacji takich świadczeń dla osób trzecich, MPM ma prawo odmówić zrealizowania takiego żądania.

**Czy MPM może pobrać opłatę za zrealizowanie uprawnienia osoby?**

Co do zasady, komunikacja z pacjentem w sprawach związanych z realizowaniem jego uprawnień wynikających z RODO, powinna być prowadzona nieodpłatnie. Gdy jednak żądania pacjenta są ewidentnie nieuzasadnione lub nadmierne, MPM może pobierać rozsądną opłatę, uwzględniającą faktycznie poniesione koszty, takie jak wydatki związane ze sporządzaniem wydruków, kserokopii czy wysyłką.

Jeśli MPM otrzymuje zapytania od jednego pacjenta w sposób ustawiczny, udzielanie odpowiedzi angażuje wielu pracowników MPM lub też prawo ma zostać zrealizowane poprzez wysyłkę informacji do pacjenta kurierem, MPM może pobrać rozsądną opłatę za realizację uprawnienia pacjenta wynikającego z RODO.

**Jak i kiedy należy realizować obowiązek informacyjny?**

Prawo pacjenta do bycia poinformowanym jest jednym z najważniejszych elementów przetwarzania danych, gwarantuje bowiem należytą przejrzystość prowadzonych przez MPM działań.

Obowiązek informacyjny należy spełnić przed rozpoczęciem przetwarzania danych,
tj. zanim dane będą zbierane. Zgodnie z RODO należy przekazać przede wszystkim takie informacje jak: oznaczenie MPM oraz dane kontaktowe MPM i wyznaczonego inspektora ochrony danych, cel przetwarzania danych oraz podstawę prawną takiego przetwarzania, jak również informacje o odbiorcach danych (np. informacja
o powierzaniu danych do laboratoriów). Pełny zakres informacji, które należy przekazać, zawiera art. 13 i 14 RODO.

Obowiązek można spełnić poprzez umieszczenie powyższych informacji
w dokumentach przekazywanych pacjentowi do podpisu, umieszczenie klauzul informacyjnych na tablicach informacyjnych w recepcji lub też umieszczenie klauzul informacyjnych na stronach internetowych MPM. Możliwe jest także ustne przekazanie informacji podczas rozmowy telefonicznej z recepcjonistką czy też inna informacja przekazana drogą elektroniczną.

Na potrzeby rozliczalności MPM przechowuje dokumentację dot. spełnienia obowiązku informacyjnego, np. poprzez zbieranie podpisanych formularzy, na których znajduje się taki obowiązek, zdjęcia tablic informacyjnych w rejestracji, zapewnienie konieczności odsłuchania nagrania podczas rozpoczęcia rozmowy telefonicznej lub też kopię strony internetowej, na której widnieje klauzula informacyjna. Działania te mają na celu udowodnienie, że właściwie spełniono obowiązki informacyjne wobec pacjenta.

RODO przewiduje sytuacje, w których przekazanie informacji dotyczących przetwarzania danych nie będzie konieczne. MPM nie musi przekazywać wszystkich powyższych informacji jeśli pacjent już te informacje posiada. Jeśli MPM zbiera dane osobowe, ale nie bezpośrednio od osoby, której dane dotyczą (np. kiedy otrzymuje udostępnioną przez inną placówkę dokumentację pacjenta lub zbiera dane osobowe osób upoważnionych przez pacjenta), spełnienie obowiązku również nie będzie konieczne, bowiem zgodnie z art. 14 ust. 5 lit. c) zbieranie takich danych uregulowane jest przepisami ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

W sytuacji ratowania życia i zdrowia, MPM również nie ma obowiązku spełniania obowiązków informacyjnych. W takim przypadku najważniejsza jest pomoc osobie, która jej potrzebuje.

**Co to jest prawo dostępu do danych i jak należy je realizować?**

Każdy pacjent oraz osoby, których dane osobowe przetwarza MPM, ma prawo uzyskać od MPM potwierdzenie czy przetwarza jego dane osobowe. Jeśli MPM rzeczywiście przetwarza te dane, osoby te mają prawo dostępu do tych danych i uzyskania wielu informacji, m.in. o celu przetwarzania jego danych, kategorii danych (np. imię, nazwisko, adres e-mail, informacje o stanie zdrowia), przysługujących uprawnieniach, odbiorcach danych czy planowanym okresie przetwarzania danych. Pełna lista informacji, o które może prosić pacjent określa art. 15 RODO.

Prawo pacjenta do dostępu do danych na podstawie RODO jest uprawnieniem odrębnym od tego, który przysługuje mu na podstawie przepisów regulujących działalność medyczną MPM. Placówki medyczne udostępniają zatem dane osobowe dotyczące pacjentów na podstawie:

* art. 15 RODO realizując prawo dostępu przysługujące osobie, której dane dotyczą.
Na podstawie tego artykułu pacjent ma prawo do otrzymania informacji na temat danych osobowych przetwarzanych na jego temat w MPM oraz do kopii tych danych.
* art. 9 UPPiRPP realizując prawo pacjenta do informacji.
* art. 26 UPPIRPP realizując prawo pacjenta do dokumentacji medycznej

W celu prawidłowego zabezpieczenia danych osobowych przed udostępnieniem osobie nieuprawnionej, ADO musi ustalić, kto i na jakiej podstawie może otrzymać dane osobowe przetwarzane w jego placówce, na jakich zasadach będzie się odbywało udostępnienie oraz w jakiej formie dane osobowe będą przekazywane. W tym celu dobrą praktyką jest opracowanie i wprowadzenie dwóch instrukcji:

1. dotyczącą udzielania informacji na temat stanu zdrowia pacjenta oraz udostępniania dokumentacji medycznej pacjenta
2. dotyczącą dostępu do danych osobowych, przysługującemu osobie, której dane dotyczą, w tym dostarczenia osobie, której dane dotyczą kopii danych osobowych podlegających przetwarzaniu

|  |  |  |
| --- | --- | --- |
|  | **RODO** | **UOPPiRPP** |
| Komu | Osobie, której dane dotyczą. | Pacjentowi, przedstawicielowi ustawowemu, osobie upoważnionej przez pacjenta, podmiotom wskazanym na podstawie ustawy.Uwaga: w przypadku wydania recept wystawianych bez dokonania osobistego badania pacjenta należy pamiętać o tym, że taka recepta może zostać wydana pacjentowi, osobom upoważnionym przez pacjenta (wskazanym z imienia i nazwiska) oraz dowolnej osobie trzeciej – jeżeli pacjent w upoważnieniu zapisze, że ww. receptę można wydać dowolnej osobie, która się po nią zgłosi. |
| Zakres danych | Wszelkie informacje dotyczące konkretnego pacjenta wraz z informacjami o celu przetwarzania, czasie, w którym dane są przechowywane, przysługujących uprawnieniach, a także fakcie przekazania danych odbiorcom (np. na podstawie umowy powierzenia). | Dokumentacja medyczna. |
| Sposób udostępnienia | Wgląd, kopia. | Wgląd, oryginał (w przypadkach określonych w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta), wyciąg, odpis, kopia |
| Sposób przekazania | Odbiór osobisty, przesłanie pocztą, kurierem, przekazanie drogą elektroniczną (zapewniającą bezpieczną komunikację), umożliwienie wglądu poprzez własny kanał do pobrania danych. | Odbiór osobisty, przesłanie pocztą, kurierem, przekazanie drogą elektroniczną (zapewniającą bezpieczną komunikację), na nośniku danych. |
| Koszt udostępnienia | Pierwsza kopia nieodpłatnie, możliwość pobierania opłaty wynikająca z kosztów administracyjnych za kolejne kopie. | UoPPiRPP określa konkretne kwoty za udostępnienie dokumentacji medycznej. |
| Udokumentowanie udostępnienia | Każde udostępnienie danych osobowych powinno być udokumentowane w sposób pozwalający na ustalenie komu kiedy, przez kogo i jakie dane zostały przekazane. | Udostępnienie dokumentacji medycznej powinno być udokumentowane przed ADO. Przepisy sektorowe określają w jaki sposób ADO powinien dokumentować udostępnienie danych osobowych w zależności od rodzaju dokumentacji medycznej. Na podstawie art. 27, ust. 4 UoPPiRPP ADO zobowiązany jest do prowadzenia wykazu dotyczącego udostępnionej dokumentacji medycznej, w którym zawarte będą następujące informacje:1) imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna;2) sposób udostępnienia dokumentacji medycznej;3) zakres udostępnionej dokumentacji medycznej;4) imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna oraz ew. nazwę uprawnionego organu lub podmiotu; 5) imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną;6) datę udostępnienia dokumentacji medycznej.Art. 42 ust. 5 Ustawy o zawodach lekarza i lekarza dentysty z kolei, reguluje kwestię udokumentowania wydawania recepty bez dokonania osobistego badania pacjenta – i wskazuje, że w takim przypadku informacja o osobie, której przekazano taką receptę lub zlecenie, odnotowuje się w dokumentacji medycznej pacjenta albo dołącza do tej dokumentacji. |

Przekazanie pacjentowi kopii danych nie stanowi podstawy do ich usunięcia
czy skrócenia ustawowych okresów ich archiwizowania.

Ponadto należy pamiętać, że każde udostępnienie danych osobowych, nie zależnie
od formy i sposobu ich przekazania ,powinno zostać udokumentowane w placówce.

**Przykład 1: Upoważnienie do dokumentacji medycznej zawiera:**

imię i nazwisko oraz datę urodzenia osoby upoważnionej przez pacjenta, zakres dokumentacji której dotyczy upoważnienie, np. dokumentacja poradni neurologicznej [nazwa placówki], wyniki badań laboratoryjnych albo opis RTG kolana.

**Przykład 2**: **Instrukcja udostępniania dokumentacji medycznej pacjenta zawiera:**

1. Informacje o tym komu można udostępnić dokumentację medyczną;
2. Na jakiej podstawie MPM udostępnia dokumentację medyczną, np. na podstawie pisemnego wniosku;
3. W jakiej formie MPM udostępnia dokumentację;
4. Udostępnienie oryginału dokumentacji;
5. MPM określa zasady udostępniania dokumentacji za pośrednictwem środków komunikacji elektronicznej lub na informatycznym nośniku danych (sposoby weryfikacji wnioskodawcy, bezpieczny sposób przekazania danych);
6. ADO musi także określić zasady dotyczące fizycznego przekazania dokumentacji medycznej, tzn. czy dopuszcza przesyłanie dokumentacji za pomocą poczty
lub kuriera, jeżeli tak to musi określić w jaki sposób będzie weryfikował odbiorcę;
7. MPM określa dodatkowo sposób weryfikacji wnioskodawcy i jego uprawnień
do dokumentacji medycznej;
8. Niezależnie od formy i sposobu udostępnienia oraz zakresu dokumentacji MPM prowadzi wykaz każdej udostępnionej dokumentacji medycznej;

Powyższa instrukcja musi być zgodna z obowiązującymi przepisami prawa
i uwzględnia rozdział 7 Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

Przykład 3: Przekazanie informacji na temat pacjenta drogą telefoniczną:

Ze względów bezpieczeństwa żadne informacje medyczne nie powinny być przekazywane telefonicznie (ani pacjentom, ani osobom upoważnionym). Nigdy nie mamy pewności, kto jest po drugiej stronie słuchawki i czy nie podszywa się pod pacjenta. W sytuacji wyjątkowej, w której placówka przekazuje telefonicznie wyniki badań lub inne informacje dotyczących danego pacjenta, konieczne będzie każdorazowe potwierdzenie, że osoba, z którą prowadzona jest rozmowa telefoniczna, jest tą, za którą się podaje. Weryfikacja może być przeprowadzona przez zobowiązanie pacjenta do podania informacji, która pozwoli na jego jednoznaczne zidentyfikowanie (np. daty urodzenia, adresu zamieszkania, ustalonego wcześniej „słowa – klucz”).

**Czy prawo do uzyskania kopii danych jest tym samym co prawo dostępu do dokumentacji medycznej?**

Prawo pacjenta dotyczące dostępu do dokumentacji medycznej nie jest tym samym co przysługujące każdemu z nas na mocy RODO prawo otrzymania kopii danych osobowych. Są to dwa różne prawa i służą różnym celom.

Oznacza to, że jeżeli pacjent wskaże, że wnioskuje o realizację prawa na gruncie przepisów RODO, to ma prawo bezpłatnie otrzymać kopię danych osobowych zawartych w dokumentacji medycznej. W takiej sytuacji pacjent nie będzie mógł jednak prosić o kopię nośnika, na którym te informacje się znajdują, np. kserokopii dokumentacji.

Jednak jeśli pacjent wnioskuje o udostępnienie kopii dokumentacji medycznej, to placówce medycznej przysługuje prawo do pobierania opłat za kserokopie dokumentacji medycznych, zgodnie z ustawą o prawach pacjenta i Rzeczniku Praw Pacjenta.

**Czy pacjent ma prawo sprostować jego dane?**

Zgodnie z RODO każdy pacjent ma prawo żądać sprostowania danych, które
są nieprawidłowe. Może również prosić o uzupełnienie danych, które są niekompletne.

Pacjent o imieniu Jan Kowalski prosi o zmianę jego imienia i nazwiska na fikcyjne Julia Kowalska. MPM może odmówić sprostowania takiej informacji bez potwierdzenia tak znaczącej zmiany danych, upewniając się czy nowo podane dane są prawdziwe.

Kiedy MPM poprawi jakąś informację dotyczącą pacjenta, powinien poinformować
o tym fakcie wszystkich odbiorców danych, w tym podmioty, którym powierzono dane osobowe. Ma to szczególne znaczenie w sytuacji, w której przekazania tych nowych informacji może mieć znaczenie dla leczenia tego pacjenta.

**Prawo do bycia zapomnianym – czy można zapomnieć pacjenta?**

Każda osoba, której dane są przetwarzane, ma prawo do żądania usunięcia swoich danych. RODO wskazuje jednak, że prawo to nie będzie miało zastosowania jeśli przetwarzanie tych danych jest niezbędne do realizacji obowiązku prawnego. Wobec faktu, że dane medyczne pacjentów przetwarzane są na podstawie stosownych przepisów prawa, dane pacjenta oraz jego dokumentacja medyczna nie będą mogły zostać usunięte na wniosek pacjenta.

Jeśli podstawą przetwarzania jest zgoda pacjenta (np. kiedy pozyskujemy jego zgodę na przesyłanie informacji marketingowych), pacjent może wycofać zgodę i zawnioskować o usunięcie jego danych. Wtedy MPM usuwa te dane i nie wykorzystuje ich już do dalszego przetwarzania w celu, dla którego zostały zebrane.

Dane mogą jednak zostać zachowane w MPM jeśli będzie to niezbędne dla celów archiwalnych (przechowywanie dokumentacji medycznej przez okres określony w przepisach prawa) bądź związanych z dochodzeniem roszczeń przez pacjenta (w ramach usprawiedliwionego interesu MPM). Dobrą praktyką po usunięciu danych zgodnie z żądaniem pacjenta, jest zachowanie informacji o tym, kto złożył wniosek i w sposób MPM wykonał żądanie. Będzie to konieczne do zachowania rozliczalności. Wyznaczony przez MPM inspektor ochrony danych, uwzględniając formy przetwarzania danych, ustala sposób rozpatrywania oraz okres przechowywania takich wniosków.

**Czy pacjent może ograniczyć przetwarzanie danych?**

Pacjent ma prawo oczekiwać, że MPM ograniczy przetwarzanie jego danych osobowych na przykład w sytuacji, w której pacjent kwestionuje prawidłowość danych przetwarzanych przez MPM. Ograniczenie oznacza w praktyce, że nie można dokonywać na danych innych operacji niż przechowywanie.

W praktyce funkcjonowania MPM do takiej sytuacji jednak nie powinno dochodzić. RODO upoważnia do dalszego przetwarzania danych mimo zgłoszonego wniosku
o ograniczenie, jeśli uzasadnia to interes publiczny nadrzędny wobec uprawnienia osoby. Ograniczenie przetwarzania danych zawartych w dokumentacji medycznej mogłoby nieść duże ryzyko dla zdrowia i życia pacjenta, z tego powodu, wobec danych medycznych, prawo do ograniczenia przetwarzania co do zasady nie będzie miało zastosowania.

**Sprzeciw i przeniesienie danych – czy MPM to dotyczy?**

Prawa pacjenta do sprzeciwu i do przeniesienia danych nie stosuje się do operacji przetwarzania, których podstawą jest obowiązek wynikający z przepisu prawa. Pacjent nie będzie miał zatem prawa do sprzeciwu wobec przetwarzania danych medycznych. Nie będzie mógł również skorzystać z prawa do przeniesienia tych danych wobec tych danych.

Prawo do przeniesienia danych będzie oczywiście przysługiwało w sytuacji kiedy podstawą przetwarzania danych będzie zgoda (np. kiedy wykorzystywane są dane kontaktowe pacjenta w celach marketingowych) oraz kiedy dane będą przetwarzane w sposób zautomatyzowany (prawo nie znajdzie więc zastosowania wobec dokumentów papierowych). W takiej sytuacji MPM zobowiązane będzie do przetwarzania danych zebranych na podstawie zgody w powszechnie używanym formacie umożliwiającym maszynowy odczyt i przeniesienie (np. otwarte formaty takie jak XML, JSON, CSV). Dane mogą zostać dostarczone do pacjenta lub do innego administratora – zgodnie z decyzją pacjenta. Więcej informacji na temat tego uprawnienia zawierają Wytyczne WP242 Grupy Roboczej Art. 29 (dostępne na stronie PUODO: <https://uodo.gov.pl/pl/10/6>).

|  |
| --- |
| ***Podstawy prawne RODO:******Artykuł 12 Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą****1.* *Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem - w szczególności gdy informacje są kierowane do dziecka - udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15-22 i 34 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.**2. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15-22. W przypadkach, o których mowa w art. 11 ust. 2, administrator nie odmawia podjęcia działań na żądanie osoby której dane dotyczą pragnącej wykonać prawa przysługujące jej na mocy art. 15-22, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.**3. Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15-22. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.**4. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.**5. Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:**a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo**b) odmówić podjęcia działań w związku z żądaniem.**Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.**6. Bez uszczerbku dla art. 11, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15-21, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.**7. Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 13 i 14, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego.**8. Komisji przysługuje prawo przyjmowania aktów delegowanych zgodnie z art. 92 w celu określenia informacji przedstawianych za pomocą znaków graficznych i procedur ustanowienia standardowych znaków graficznych.****Artykuł 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) 29 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 informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.**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 informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.**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 w powszechnie stosowanej formie elektronicznej.**4. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.****Artykuł 16 Prawo do sprostowania 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.****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.****Artykuł 20 Prawo do przenoszenia danych****1. 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, jeżeli:**a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz**b) przetwarzanie odbywa się w sposób zautomatyzowany.**2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.**3. Wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla art. 17. 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.**4. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.****Artykuł 21 Prawo do sprzeciwu****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.* |

1. **PRAWA PACJENTA**

**Jakie prawa posiada pacjent na mocy przepisów regulujących świadczenie usług medycznych?**

**Prawo pacjenta do tajemnicy informacji z nim związanych.**

Prawo to zobowiązuje wszystkie osoby zatrudnione w MPM, które wykonują zawód medyczny i udzielają świadczenia zdrowotnego pacjentowi, do zachowania w tajemnicy informacji związanych z pacjentem. Ponadto do zachowania w tajemnicy obowiązane
są także rejestratorki medyczne, osoby zajmujące się statystyką medyczną/rozliczeniami z NFZ, informatycy oraz wszelkie osoby, które z upoważnienia administratora mają dostęp do informacji na temat pacjenta. Wszystkie powyższe osoby obowiązane są tajemnicą także po śmierci pacjenta.

**Prawo do poszanowania intymności i godności pacjenta**

Pacjent może zażyczyć sobie, żeby przy udzielaniu świadczeń zdrowotnych była obecna wskazana przez niego osoba bliska (żona/mąż, rodzice, dziadkowie, dzieci, wnuki, teściowie, opiekun prawny, konkubent/konkubina oraz dowolna osoba wskazana przez pacjenta). Prawo to wiąże się z możliwością przekazywania, np. podczas wizyty lekarskiej, informacji zarówno pacjentowi jak i osobie trzeciej. W celu uniknięcia sytuacji, w której pacjent oskarżyłby lekarza/pielęgniarkę o udzielenie informacji na temat swojego stanu zdrowia osobie bliskiej, lekarz/pielęgniarka MPM odnotowują, jeszcze przed wprowadzeniem innych zapisów w dokumentacji medycznej, że na życzenie pacjenta towarzyszy mu osoba bliska, która tym samym będzie świadkiem przekazywania pacjentowi wszelkich informacji związanych z procesem jego leczenia.

Ponadto, w przypadku odmowy obecności osoby bliskiej przy udzielaniu świadczeń zdrowotnych (w przypadkach określonych w art. 21 ust 2 ustawy o prawach pacjenta
i Rzeczniku Praw Pacjenta), osoba wykonująca zawód medyczny odnotowuje ten fakt
w dokumentacji medycznej.

**Prawo pacjenta do dokumentacji medycznej**

Pacjent, jego przedstawiciel ustawowy lub osoba upoważniona przez pacjenta, mają prawo uzyskać dostęp do dokumentacji medycznej w wybrany przez siebie sposób
(tj. poprzez wgląd, otrzymanie odpisów, wypisów, kopii, oryginału – w tej ostatniej formie jedynie w sytuacjach narażenia życia lub zdrowia).

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). [↑](#footnote-ref-1)
2. Podmiot leczniczy oraz lekarz lub pielęgniarka wykonujący zawód w ramach działalności leczniczej jako praktykę zawodową, o których mowa w przepisach ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej. [↑](#footnote-ref-2)
3. 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. [↑](#footnote-ref-3)
4. Organ nadzorczy odpowiedzialny za kontrolę przestrzegania RODO na terytorium RP. [↑](#footnote-ref-4)
5. Stanowisko dotyczące ważności zgód na przetwarzanie danych osobowych, <https://giodo.gov.pl/pl/1520281/10303> [↑](#footnote-ref-5)
6. Żywotne interesy osoby, której dane dotyczą, należy rozumieć jako interesy niezbędne dla życia tej osoby. [↑](#footnote-ref-6)
7. Rzecznik Praw Pacjenta zauważa, że wskazanie konkretnej liczby dni jest utrudnianiem dostępu pacjenta do dokumentacji medycznej. Każdy wniosek powinien być rozpatrywany indywidualnie. [↑](#footnote-ref-7)
8. Art. 24 ust. 2 pkt 1 i 2 Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta [↑](#footnote-ref-8)
9. Więcej informacji na temat oceny skutków dla ochrony danych znajdujące się w Wytycznych WP248 Grupy Roboczej Art. 29, dostępnych na stronie Urzędu Ochrony Danych Osobowych. [↑](#footnote-ref-9)
10. Więcej na temat uprzednich konsultacji na: https://uodo.gov.pl/pl/127 [↑](#footnote-ref-10)
11. Przykładowy rejestr czynności przetwarzania danych osobowych oraz wskazówki dot. prowadzenia rejestru znajdują się na stronie Urzędu Ochrony Danych Osobowych: https://uodo.gov.pl/pl/123/214 [↑](#footnote-ref-11)
12. Więcej informacji na temat zadań o statusu IOD dostępnych jest na stronie Urzędu Ochrony Danych Osobowych – www.uodo.gov.pl [↑](#footnote-ref-12)