Polityka Ochrony Danych Osobowych Dental Art.

14.10.2019r.

Niniejsza Polityka Ochrony Danych Osobowych w Dental Art. jest dokumentem opisującym zasady i procedury ochrony danych osobowych stosowane przez Administratora, w celu

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

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych w Dental Art. odbywa się zgodnie z powyższym Rozporządzeniem.

Opisane i zastosowane w niej zabezpieczenia i rozwiązania organizacyjne mają na celu zapewnienie, że dane osobowe są przetwarzane (Motyw 39 oraz art.5.RODO):

- w sposób rzetelny oraz zgodnie z prawem,
- w konkretnych, wyraźnie określonych i uzasadnionych celach,
- adekwatnie oraz stosownie do celów, w których są przetwarzane- minimalizacja danych,
- prawidłowo i w razie potrzeby uaktualniane,
- przechowywane przez okres nie dłuższy, niż jest to niezbędne do osiągnięcia celów, w których te dane są przetwarzane,
- w sposób zapewniający bezpieczeństwo danych osobowych.

Administratorem danych osobowych jest Dental Art. Prywatna Praktyka Dentystyczna Andrzej Wawrzyniak, z siedzibą ul. Polna 5, 62-020 Swarzędz, NIP 777 28 63 408, reprezentowana przez Andrzeja Wawrzyniaka, właściciela.

Podstawy prawne:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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),

2. Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. t.j. Dz. U. z 2016 r. poz. 1638, 1948, 2260, z 2017 r. poz. 2110, 2217).
3. Ustawa z dnia 06 kwietnia 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2017 r. poz. 1318, 1524),
4. Ustawa z dnia 21 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. 2017 tj. poz.1845),
5. Niniejsza Polityka Ochrony Danych Osobowych.

DEFINICJE:

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46.

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby fizycznej.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Profilowanie – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Anonimizacja- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych.

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Zbiór danych- zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów,

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Podmiot przetwarzający (**Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiot danych - każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące życia seksualnego osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Spis treści:

3. *Upoważnienia do przetwarzania danych osobowych*
4. *Poufność procesu przetwarzania danych*
5. *Współpraca z podmiotami zewnętrznymi*
6. *Udostępnianie danych osobowych*
7. *Uprawnienia osób, których dane osobowe są przetwarzane w podmiocie leczniczym*

II Ryzyko w podmiocie leczniczym:

1. *Analiza ryzyka*
2. *Ocena skutków dla systemu ochrony danych*
3. *Zarządzanie ryzykiem*

III Inspektor Ochrony Danych

IV Rejestr czynności przetwarzania

V Instrukcja postępowania w przypadku naruszenia systemu ochrony danych osobowych

VI Procedury przywrócenia dostępności danych osobowych w razie wystąpienia incydentu fizycznego lub technicznego

VII Kontrole wewnętrzne i audyty bezpieczeństwa

VIII Postępowanie dyscyplinarne

IX Szkolenia personelu

X Wykaz zabezpieczeń

XI Zasady zarządzania systemem informatycznym

I. Weryfikacja posiadanych danych osobowych i zasady ich przetwarzania

1. Inwentaryzacja danych

1.1 Poprzez dane osobowe w podmiocie leczniczym, zgodnie z art. 4 pkt 1) RODO należy rozumieć wszystkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można w sposób pośredni lub bezpośredni zidentyfikować, z uwzględnieniem identyfikatorów. Dane te mogą dotyczyć pracowników podmiotu leczniczego, jego pacjentów lub osoby współpracujące z podmiotem leczniczym.

1.2 Dane osobowe w podmiocie leczniczym zorganizowane są w struktury, za pomocą których Administrator może ocenić ryzyko ich przetwarzania oraz ocenić konieczność przeprowadzenia procedury oceny skutków dla systemu ochrony danych, o którym mowa w art. 35 RODO po 25 maja 2018 r.

1.3 Dane osobowe opisane są z uwzględnieniem, co najmniej poniższych informacji:

a) Nazwa przetwarzanych danych osobowych,
b) Cele przetwarzania,
c) Zakres przetwarzania,
d) Odbiorcy danych,
e) Zakres czynności przetwarzania,

f) Zasoby służące do przetwarzania danych osobowych,
g) Informacja o konieczności wpisu do rejestru czynności przetwarzania,
h) Informacja o konieczności przeprowadzenia oceny skutków dla ochrony danych na zbiorze,
i) Okres przechowywania.

1.4 Szczegółowo opis danych osobowych został przedstawiony w załączniku nr 1.

2 .Legalność procesu przetwarzania danych osobowych

2.1 Administrator swoimi działaniami i organizacją podmiotu leczniczego zapewnia, że:

a) dane osobowe w podmiocie leczniczym przetwarzane są w sposób legalny, na podstawie art. 6 ust. 1 ppkt. b), c) i d) oraz art. 9 ust. 2 ppkt c) i h) RODO w związku z art. 3 ust. 1 i 2 ustawy o działalności leczniczej oraz art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, a także w związku z art. 54 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa lub innych właściwych przepisów z zakresu prawa ubezpieczeń społecznych. Zgoda na przetwarzanie danych osobowych może zostać pozyskana w inny sposób, ale musi ona spełniać przesłanki, o których mowa w art. 7 ust. 1 RODO,
b) zakres pozyskiwanych danych wynika z przepisów prawa, o których mowa w punkcie 2.1 a) niniejszego dokumentu i jest adekwatny do zdefiniowanych celów przetwarzania,
c) określono konkretny czas przez jaki dane są przetwarzane (załącznik nr 1),
d) wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny, zgodnie z art. 12-14 RODO, a wzór klauzul informacyjnych znajduje się w załączniku 1 b,
e) obowiązek informacyjny wobec pacjentów podmiotu leczniczego może być wykonywany poprzez umieszczenie na tablicy informacyjnej przy stanowisku rejestracyjnym i w poczekalni stosownych tablic.

f) z wszystkimi współpracującymi podmiotami gospodarczymi podpisano, na mocy art. 28 RODO, umowy powierzenia przetwarzania danych osobowych lub w umowach podstawowych wprowadzono uregulowania odnoszące się do obowiązków zapewnienia przestrzegania przepisów RODO przez te podmioty,
g) jeżeli dane osobowe zostały pozyskane nie bezpośrednio od osób, których dotyczą, administrator musi je o tym powiadomić w sposób umożliwiający im niepodważalne powzięcie takiej wiedzy.

2.2 Dane osobowe w podmiocie leczniczym są pozyskiwane bezpośrednio od pacjentów lub od innych podmiotów uczestniczących w udzielaniu tym pacjentom świadczeń zdrowotnych.

3. Upoważnienia do przetwarzania danych osobowych:

3.1 Administrator do przetwarzania danych osobowych w podmiocie leczniczym dopuszcza jedynie osoby posiadające stosowane upoważnienia. Wzór stosownych upoważnień stanowi Załącznik nr 1 c.
3.2 Administrator jest odpowiedzialny za proces nadawania i wycofywania upoważnień do przetwarzania danych osobowych w podmiocie leczniczym.
3.3 Zmiana uprawnień w zakresie przetwarzania danych osobowych odbywa się na wniosek bezpośredniego przełożonego, za wiedzą Inspektora Ochrony Danych Osobowych, zgodnie z załącznikiem nr 1 c.1.
3.4 W podmiocie leczniczym prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych, w sposób umożliwiający prawidłową identyfikację historii i prawidłowości procesu przetwarzania danych osobowych. Rejestr jest prowadzony na druku zgodnym z załącznikiem nr 1 d.

4. Poufność procesu przetwarzania danych osobowych.

4.1 Każda z osób dopuszczona do przetwarzania danych osobowych lub współpracująca z podmiotem leczniczym jest zobowiązana do:

a) przetwarzania danych osobowych jedynie w zakresie i jedynie w celu w jakim zostało im wydane upoważnienie lub podpisano umowę powierzenia przetwarzania danych osobowych,

b) zachowania w tajemnicy informacji i danych osobowych, do których posiada dostęp,

c) niewykorzystywania dostępnych danych osobowych do celów sprzecznych z zakresem upoważnienia lub umowy powierzenia przetwarzania danych osobowych.

d) zachowania poufności procesów i metod zabezpieczeń danych osobowych w podmiocie leczniczym.

e) ochrony informacji i danych osobowych przed przypadkowym, niepożądanym ujawnieniem, modyfikacją, utratą, zniszczeniem danych osobowych czy też nieuprawnionym dostępem osób niepożądanych.

4.2 Osobami, które mogą być dopuszczone do przetwarzania danych osobowych w podmiocie leczniczym mogą być (poza kryterium zatrudnienia lub współpracy z podmiotem leczniczym):

4.2.1 przedstawiciele zawodów medycznych, z zastrzeżeniem art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

4.2.2 personel pomocniczy przy udzielaniu świadczeń zdrowotnych, a także osoby odpowiedzialne za czynności związane z prawidłowym funkcjonowaniem systemów teleinformatycznych, w których przetwarzana jest dokumentacja medyczna,

4.3 Osoby dopuszczone do przetwarzania danych osobowych w podmiocie leczniczym, przed przystąpieniem do pracy, powinni odbyć szkolenie z zasad ochrony danych osobowych w podmiocie leczniczym, o którym mowa szerzej w Rozdziale IX.

4.4 Osoby, które zostają dopuszczone do przetwarzania danych osobowych, a które zapoznały się treścią niniejszej Instrukcji są zobowiązane do podpisania tzw. oświadczenia o poufności, którego wzór stanowi załącznik nr 1 e.

4.5 W podmiocie leczniczym zabronione jest udzielanie wszelkich informacji zawierających dane osobowe osobom, których tożsamości nie można zweryfikować.

Weryfikacja tożsamości może odbywać się poprzez żądanie okazania dokumentu tożsamości lub innego dokumentu zawierającego zdjęcie wnioskodawcy lub poprzez wykorzystanie informacji zawartej w dokumentacji medycznej, która jest znana jedynie wnioskodawcy. Do tego celu należy wykorzystać metodę pytań bezpośrednich, w których wnioskodawca udzieli poprawnych informacji w co najmniej dwóch zapytaniach.

4.6 W podmiocie leczniczym niedopuszczalne jest przekazywania wszelkich informacji zawierających dane osobowe podmiotom, instytucjom czy też organom, które nie mogą się wykazać prawidłową podstawą prawną dostępu do danych osobowych.

4.7 W przypadku konieczności wydania dokumentów zawierających dane osobowe (np. wynik badań, recepty itp.) należy każdorazowo weryfikować tożsamość odbierającego za pomocą mechanizmu, o którym mowa w punkcie 4.5, a w przypadku, kiedy odbierającym nie jest adresat dokumentu należy zażądać upoważnienia. Za skuteczne uznaje się upoważnienie wpisane przez pacjenta do jego karty, bądź upoważnienie notarialne. Pracownicy podmiotu proszeni są o zwrócenie uwagi pacjenta na możliwość wpisywania na swojej karcie osób upoważnionych.

4.8 W podmiocie leczniczym zakazuje się wywoływania pacjentów z użyciem ich imion i nazwisk i wprowadza się system ich anonimizacji (godzina umówionej wizyty).

4.9 Organizacja rejestracji i poczekalni podmiotu leczniczego umożliwia zachowanie poufności osobom przebywającym bezpośrednio przy rejestracji.

4.10 Udzielanie świadczeń zdrowotnych w podmiocie leczniczym odbywa się w miejscach specjalnie do tego wyznaczonych. Zabrania się udzielania informacji dotyczących pacjentów na korytarzach, w poczekalni lub innych nieprzystosowanych do tego miejscach w podmiocie leczniczym.

4.11 Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, tablicach korkowych, parapetach, gablotach itp.

4.12 Wydruki i inne dokumenty zawierające dane osobowe są przechowywane w specjalnie do tego celu przeznaczonych metalowych szafach zamykanych na klucz. Na stanowiskach pracy mogą być dostępne jedynie dokumenty dotyczące danej sprawy/ danego pacjenta. Stosowana jest zasada tzw. czystego biurka.

4.13 Po zakończeniu pracy wszelka dokumentacja zawierająca dane osobowe jest przechowywana w szafach zamykanych na klucz lub w pomieszczeniach o ograniczonym dostępie osób postronnych, do których dostęp jest utrudniony poprzez zastosowanie zabezpieczeń fizycznych takich jak: zamki w drzwiach.

4.14 Wszelkie dokumenty zawierające dane osobowe niszczone są z użyciem niszczarki.

4.15 Zaleca się zwrócenie szczególnej uwagi pracownikom podmiotu leczniczego na sytuację przypadkowego pozostawienia dokumentów zawierających dane osobowe w miejscach ogólnodostępnych.

4.16 Administrator jest zobowiązany do corocznej weryfikacji posiadanych zbiorów danych osobowych, które mają na celu wyeliminowanie danych, dla których ustały podstawy przetwarzania.

5. Współpraca z podmiotami zewnętrznymi

5.1 W działalności podmiotu leczniczego jest dopuszczalna współpraca z podmiotami zewnętrznymi, którym udostępnia się dane osobowe, których Administratorem jest Dental Art.

5.2 Powierzenie przetwarzania danych osobowych może odbywać się jedynie na podstawie umowy lub innego instrumentu prawnego, zgodnie z zasadami określonymi w art. 28 RODO.

5.3 W podmiocie leczniczym prowadzona jest ewidencja podmiotów, z którymi podpisano umowy powierzenia, którego wzór stanowi załącznik nr 1 f.

5.4 Ewidencja ta zawiera, co najmniej:

a) nazwę, adres siedziby i dane kontaktowe podmiotu,

b) datę podpisania umowy,

c) przedmiot umowy,

d) informacja o rodzajach zbiorów, które obejmuje umowa przetwarzania.

5.5 Podmiot leczniczy może również współpracować z podmiotami, w których to podmiot leczniczy jest podmiotem przetwarzającym, jeżeli podpisał stosowną umowę w tym zakresie.

5.6 Zaleca się szczególną ostrożność w zakresie sposobów dokumentowania współpracy, o której mowa w punkcie 5.5. Należy bowiem zachować maksymalną możliwość anonimizowania tej współpracy, a jeśli to niemożliwe należy korzystać z narzędzi informatycznych i technicznych zapewniających szyfrowane połączenia w zakresie przekazywania informacji zawierających dane osobowe. W przypadku przekazywania informacji drogą poczty tradycyjnej należy zastosować postanowienia punktu 6.7 niniejszej instrukcji.

6. Udostępnianie danych

6.1 Podmiot leczniczy udostępnia dane osobowe jedynie na podstawie obowiązujących przepisów prawa i w granicach prawa.

6.2 Dane osobowe pacjentów, które znajdują się w dokumentacji medycznej są udostępniane na zasadach, w trybie i na sposób określony w przepisach art. 26 i 27 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

6.3 Ewidencja udostępnionej dokumentacji medycznej prowadzona jest na podstawie art. 27 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta i zawiera, co najmniej: imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna, sposób udostępnienia dokumentacji medycznej, zakres udostępnionej dokumentacji medycznej, imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna, a w przypadkach, o których mowa w art. 26 *udostępnianie dokumentacji medycznej* ust. 3 i 4, także nazwę uprawnionego organu lub podmiotu, imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną, datę udostępnienia dokumentacji medycznej.

6.4 Wzór ewidencji, o której mowa w punkcie 6.3 stanowi załącznik nr 1g.

6.5 Podmiot leczniczy udostępnia również dane, na podstawie innych przepisów niż te, o których mowa w punkcie 6.2 jedynie na pisemny wniosek i za potwierdzeniem.

6.6 Wzór ewidencji udostępnionych danych w trybie, o którym mowa w punkcie 6.5 stanowi załącznik nr 1 h.

6.7 Podmiot leczniczy przekazując dane drogą pocztową przekazuje je listem poleconym za potwierdzeniem odbioru, w dwóch niezależnie zamkniętych kopertach.

6.8 W przypadku udostępniania dokumentów za pomocą korespondencji mailowej podmiot ma obowiązek szyfrować przekazywane pliku, zgodnie z załącznikiem nr 9. Instrukcja szyfrowania plików znajduje się w rejestracji podmiotu leczniczego.

7 Uprawnienia osób, których dane osobowe są przetwarzane w podmiocie leczniczym.

7.1 Podmiot leczniczy zapewnia osobom, których dane osobowe przetwarza do realizacji wszystkich przysługujących im praw na mocy art. 15 i 16 RODO.

7.2 Podmiot leczniczy może wprowadzić, na podstawie art. 9 ust. 1 pkt h) RODO ograniczenia w realizacji praw osób, których dane przetwarza, a wynikających z art. 17, 18, 20 i 21 RODO, szczególnie powołując się na zapisy art. 29 ustawy z dnia 06 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

7.3 W przypadku zastosowania trybu, o którym mowa w punkcie 7.2 należy taką sytuację pisemnie wyjaśnić osobie, która wniosła sprawę w zakresie realizacji jej praw.

II. Ryzyko w podmiocie leczniczym

1. Analiza ryzyka

1.1.W podmiocie leczniczym przeprowadzana jest analiza ryzyka. Analiza ryzyka może odbywać się dla wszystkich wyodrębnionych zbiorów danych osobowych lub dla procesów przetwarzania.

1.2 Analiza ryzyka przeprowadzana jest w celu określenia, oceny i minimalizacji zagrożeń, których efektem ma być wdrożenie optymalnych i adekwatnych zabezpieczeń.

1.3 Analiza ryzyka przeprowadzona jest corocznie, **nie później niż do dnia 14.10** lub w przypadku wprowadzenia nowych procedur lub rozwiązań organizacyjnych w podmiocie leczniczym, zgodnie z procedurą analizy ryzyka opisaną w Załączniku nr 2.

2. Ocena skutków dla ochrony danych osobowych

2.1 Dla zbiorów danych osobowych, w których znajdują się dane osobowe, których nieuprawnione ujawnienie wiąże się z wysokim ryzykiem uszczerbku dla osób, których dane dotyczą przeprowadzana jest ocena skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO.

2.2 Ocena skutków dla ochrony danych osobowych polega na:

a) opisie planowanych operacji i celów przetwarzania,

b) opisie i ocenie przez administratora czy planowane operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów,

c) ocenie ryzyka naruszenia praw lub wolności osób, których dane dotyczą,

d) opisie środków planowanych w celu zaradzenia ryzykiem, w tym określeniu mechanizmów, zabezpieczeń i środków technicznych, mających zapewnić bezpieczeństwo procesu,

2.3 Ocena skutków dla ochrony danych odbywa się zgodnie z procedurą opisaną w Załączniku nr 2.

3. Polityka zarządzania ryzykiem

3.1 Czynności, o których mowa w punkcie II stanowią politykę zarządzania ryzykiem w podmiocie leczniczym.

3.2 Za nadzór nad realizacją polityki zarządzania ryzykiem odpowiada Administrator.

3.3. Polityką zarządzania ryzykiem administruje wyznaczony pracownik. Analiza ryzyka i ocena skutków dla systemu ochrony danych może odbywać się przy udziale Inspektora Ochrony Danych Osobowych.

3.4 Wyznaczony pracownik ma obowiązek sporządzenia corocznego raportu związanego z ryzykiem w podmiocie leczniczym **nie później niż do dnia 14.10**.

III. Inspektor Ochrony Danych.

Z uwagi na fakt, że głównym obszarem działalności podmiotu leczniczego jest przetwarzanie danych, o których mowa w art. 9 ust. 1 RODO i polega na operacjach przetwarzania, które ze względu na swój charakter, zakres oraz cele wymagają systematycznego monitorowania tych osób, w podmiocie leczniczym wyznaczony został Inspektor Ochrony Danych.

1. Za wyznaczenie Inspektora Ochrony Danych w podmiocie leczniczym odpowiada Administrator.
2. Inspektorem Ochrony Danych w podmiocie leczniczym może być jedynie osoba, która posiada fachową wiedzę na temat prawa i praktyki w ochronie danych osobowych oraz w sektorze ochrony zdrowia.
3. Inspektor Ochrony Danych nie musi być pracownikiem podmiotu leczniczego.
4. Inspektorem Ochrony Danych w Podmiocie jest Anna Serafin.
5. Administrator jest zobowiązany do udostępnienia danych kontaktowych Inspektora Danych w sposób umożliwiający jego identyfikację i kontakt oraz jest zobowiązany powiadomić o nich organ nadzorczy.

5.1 Poprzez udostępnienie danych Inspektora Ochrony Danych należy rozumieć, co najmniej ich publikację na stronie internetowej administratora oraz w widocznym miejscu, w siedzibie administratora.

6. Administrator ma obowiązek zapewnić Inspektorowi Ochrony Danych możliwość wykonywania jego obowiązków w sposób niezależny i zapewnić mu status, o którym mowa w art. 38 RODO.

7. Zadania Inspektora Ochrony Danych:

7.1 Informowanie administratora podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i innych przepisów regulujących tą materię,

7.2 Monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów,

7.3 Podejmowanie działań zwiększających świadomość personelu podmiotu leczniczego, inicjowanie i organizowanie szkoleń personelu uczestniczącego w operacjach przetwarzania,

7.4 Przeprowadzanie wewnętrznych audytów,

7.5 Udzielanie na żądanie administratora zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z rozdziałem II niniejszego dokumentu,

7.6 Współpraca z organem nadzorczym,

7.7 Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

8. Inspektor Ochrony Danych jest wyznaczony na podstawie stosowanego zarządzenia administratora, którego wzór stanowi załącznik nr 3.

9. Dane kontaktowe Inspektora Ochrony Danych są przekazywane organowi nadzorczemu według trybu i za pomocą narzędzi opracowanych i wdrożonych przez organ nadzoru.

IV. Rejestr czynności przetwarzania

1. Dla zbiorów, w których przetwarzane są dane, o których mowa w art. 9 ust. 1 RODO prowadzony jest rejestr czynności przetwarzania.
2. Rejestr, o którym mowa w punkcie 1 niniejszego rozdziału może być również prowadzony dla innych zbiorów. Szczegółowa informacja o zbiorach, dla których prowadzony jest rejestr czynności przetwarzania zawarta jest w Załączniku nr 1.
3. Rejestr czynności przetwarzania winien zawierać co najmniej informacje, o których mowa w art. 30 RODO tj.:
   3.1 Imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
   3.2 cele przetwarzania;
   3.3 opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   3.4 kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   3.5 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;
   3.6 jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   3.7 jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
4. Rejestr czynności przetwarzania jest prowadzony w oparciu o załącznik nr 1.

V. Zasady postępowania w przypadku naruszenia systemu ochrony danych

1. Każda osoba, której administrator wydał upoważnienie do przetwarzania danych osobowych, ma obowiązek natychmiastowego powiadamiania o występującym zagrożeniu lub wystąpieniu incydentu związanego z systemem ochrony danych osobowych w podmiocie leczniczym.
2. Powiadomienie to może mieć charakter ustny lub pisemny.
3. Adresatem takiego powiadomienia jest Inspektor Ochrony Danych.
4. Po otrzymaniu takiego powiadomienia Inspektor Ochrony Danych podejmuje niezwłocznie czynności w celu ustalenia stanu faktycznego.
5. W przypadku uzasadnionego podejrzenia wystąpienia incydentu lub naruszenia systemu ochrony danych osobowych podejmuje działania mające zapobiec dalszym skutkom oraz powiadamia administratora.
6. Po dokonaniu czynności zabezpieczających, Inspektor Ochrony Danych, ma za zadanie przeprowadzić postępowanie wyjaśniające, które:
   6.1 ustali ostateczny zakres, przyczyny wystąpienia oraz skutki, zarówno dla podmiotu leczniczego, jak i osób, których dane dotyczyły,
   6.2 podejmuje niezbędne czynności mające na celu przywrócenie prawidłowości działania systemu ochrony danych osobowych w podmiocie leczniczym,
   6.3 opracowuje działania naprawcze i zapobiegawcze, których zadaniem jest wyeliminowanie niepożądanych zdarzeń w przyszłości,
   6.4 wskazuje osoby odpowiedzialne za wystąpienie sytuacji.
7. Powyższe czynności są dokumentowane przez Inspektora Ochrony Danych Osobowych za pomocą formularza, którego wzór stanowi załącznik nr 5.
8. Rejestr formularzy, o których mowa w punkcie 7 niniejszego rozdziału prowadzi Administrator.
9. Inspektor Ochrony Danych ma obowiązek przedstawienia raportu Administratorowi w czasie umożliwiającym Administratorowi powiadomienie o incydencie lub

naruszeniu systemu ochrony danych osobowych organu nadzorczego nie później niż na 72 godziny od czasu jego wykrycia.

VI. Procedury przywrócenia dostępności danych osobowych w razie wystąpienia incydentu technicznego lub fizycznego

1. Administrator wyznaczył następujące obszary krytyczne dla organizacji systemu ochrony danych osobowych:

   1.1 brak zasilania w podmiocie leczniczym,

   1.2 awaria systemu informatycznego,

   1.3 awaria sprzętu do przetwarzania danych osobowych,

   1.4 brak dostępu do sieci internetowej,

   1.5 brak dostępu do pomieszczeń, w których przetwarzane są dane osobowe.

2. Wobec zdefiniowanych obszarów krytycznych opracowano Plan ciągłości działania stanowiący Załącznik nr 6.

VII Kontrole wewnętrzne i audyty bezpieczeństwa

1. Kontrolą systemów służących do przetwarzania danych osobowych zajmuje się Inspektor Ochrony Danych.
2. Kontrole przeprowadzane są regularnie, co najmniej raz do roku, a w przypadku wystąpienia incydentu w podmiocie leczniczym, kompleksową kontrolę obejmującą wszystkie aspekty działalności rozpoczyna się nie później niż 7 dni po zakończeniu działań związanych z incydentem, który wystąpił.
3. Kontrola przeprowadzana jest z zastrzeżeniem wymogów i terminów określonych w RODO.
4. Kontrola przeprowadzana jest przy uwzględnieniu minimalnych wytycznych jakimi są: badanie pod względem zgodności z prawem, branżowymi standardami postepowania, normami i przepisami wewnętrznymi.

5. Inspektor Ochrony Danych może wykonywać kontrole osobiście, może, przy aprobacie Administratora wyznaczyć do tego inną osobę lub podmiot.
6. Kontrole przeprowadzane są na podstawie programów kontroli, w których opisywany jest ich zakres, termin, cele oraz metody ich przeprowadzania oraz doraźnie.
7. Proces kontroli musi być dokumentowany i uzupełniony pozyskaniem obiektywnych dowodów na prawidłowość procesu kontrolnego.
8. Jeśli podczas kontroli stwierdzone zostają nieprawidłowości zagrażające systemowi ochrony danych osobowych w podmiocie leczniczym, kontroler musi niezwłocznie powiadomić o tym fakcie administratora.
9. Wynik kontroli musi być udokumentowany i przekazany Administratorowi w ciągu 14 dni od jej zakończenia.
10. Wzór raportu pokontrolnego określa załącznik nr 7.
11. Administrator może zlecić badanie audytowe niezależnemu podmiotowi, po poinformowaniu o tym fakcie Inspektora Ochrony Danych.

VIII Postępowanie dyscyplinarne

1. Pracownicy podmiotu leczniczego i podmioty współpracujące mają bezwzględny obowiązek stosowania przepisów prawa i przepisów wewnętrznych obowiązujących w podmiocie leczniczym w zakresie ochrony danych osobowych.
2. W przypadku wystąpienia incydentu, naruszenia procedur czy też zaniechania czynności wynikających z obowiązków w zakresie ochrony danych osobowych, wszystkie takie czynności będą traktowane jako ciężkie naruszenie zasad i stosunków formalnych panujących w podmiocie leczniczym.
3. Administrator, jako Pracodawca, ma prawo do potraktowania działań, o których mowa w punkcie 2 powyżej jako działań podlegającej sankcjom karnym wynikającym z RODO lub innych przepisów krajowych w zakresie organizacji procesu ochrony

danych osobowych i jest uprawniony do złożenia stosownych doniesień do organów nadzorczych.

IX Szkolenia personelu

1. Każdy pracownik/ współpracownik podmiotu leczniczego, przed przystąpieniem do pracy na zbiorach danych osobowych podmiotu leczniczego musi zostać przeszkolony w zakresie przepisów związanych z ochroną danych.
2. Za przeprowadzenie szkoleń odpowiada Inspektor Ochrony Danych.
3. Każde szkolenie musi być udokumentowane listą obecności, na której poza imionami i nazwiskami jego uczestników z ich podpisami musi być opisany zakres szkolenia.
4. Inspektor Ochrony Danych przeprowadza szkolenia w miarę potrzeb, po każdej zmianie przepisów mających znaczenie dla procesów ochrony danych osobowych w podmiocie leczniczym oraz nie rzadziej niż raz na 12 miesięcy.

X Wykaz zabezpieczeń

1. W podmiocie leczniczym prowadzony jest wykaz zabezpieczeń organizacyjnych, technicznych i informatycznych, w którym w sposób usystematyzowany opisano procedury zabezpieczeń.
2. Wykaz, o którym mowa w punkcie powyżej prowadzi Administrator podmiotu leczniczego.
3. Wykaz prowadzony jest w formie papierowej i elektronicznej, zgodnie z załącznikiem nr 8.
4. Wykaz winien być aktualizowany każdorazowo po wprowadzeniu nowych rozwiązań w podmiocie leczniczym oraz po analizie ryzyka w podmiocie leczniczym, o ile jej wynik tego wymaga.

XI Instrukcja zarządzania systemem informatycznym

1. Instrukcja stanowi zestaw procedur opisujących zasady zabezpieczania danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych.
2. Za nadzór nad jej przestrzeganiem odpowiada Administrator.
3. Szczegółowo opis procedur zawarty jest w załączniku nr 9 do niniejszego dokumentu.