Polityka ochrony danych w podmiocie leczniczym Centrum Rehabilitacji FIZJOLUX

§ 1

1. Niniejsza polityka ochrony danych określa zasady przetwarzania danych osobowych w podmiocie leczniczym Centrum Rehabilitacji FIZJOLUX.
2. Użyte w niniejszej polityce ochrony danych określenia oznaczają:
    1) **Administrator** – Centrum Rehabilitacji FIZJOLUX - podmiot leczniczy FIZJOLUX Patryk Gruszczyński, adres 08-300 Sokołów Podlaski, ul. Kościuszki 13 NIP: 9591798602, REGON: 3663085500025.
    a. **Dane Osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, w tym w szczególności imię, nazwisko, adres zamieszkania lub innego miejsca pobytu, PESEL, adres poczty elektronicznej, Dane Dotyczące Zdrowia oraz inne dane określające fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
    b. **Dane Dotyczące Zdrowia** – Dane Osobowe obejmujące dane o stanie zdrowia osoby, której dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dotyczą, w tym w szczególności informacje zbierane podczas rejestracji do usług opieki zdrowotnej lub podczas udzielania świadczeń zdrowotnych, numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych, informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych, a także wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła;
    c. **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem polskim;
    d. **Pacjent** – osoba zwracająca się o udzielenie świadczeń zdrowotnych lub korzystająca ze świadczeń zdrowotnych udzielanych przez Administratora;
    e. **Personel** –osoby świadczące pracę na rzecz Administratora w ramach stosunku pracy lub umów cywilnoprawnych;
    f. **Polityka** – niniejsza Polityka ochrony danych osobowych;

g. **Procesor** – podmiot, któremu Administrator powierzył przetwarzanie Danych Osobowych;

h. **Prezes UODO** – Prezes Urzędu Ochrony Danych Osobowych będący organem publicznym właściwym w sprawach danych osobowych;

i. **Przetwarzanie** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

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

3. Administrator przetwarza Dane Osobowe z zachowaniem zasad zgodności z prawem, rzetelności i przejrzystości.
4. Dane Osobowe są zbierane i przetwarzane wyłącznie w wyraźnych i prawnie uzasadnionych celach zgodnie z zasadami ograniczenia celu oraz minimalizacji danych.
5. Administrator przechowuje Politykę w wersji elektronicznej oraz w wersji papierowej w swojej siedzibie i udostępnia ją do wglądu osobom uprawnionym do przetwarzania Danych Osobowych oraz osobom, którym takie uprawnienie ma zostać nadane przez Administratora.

§ 2.

Administrator jest podmiotem leczniczym wykonującym działalność leczniczą na podstawie ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (tekst jedn. Dz. U. z 2020 r., poz. 295 ze zm.) i przetwarza Dane Osobowe:

1) Pacjentów:
   a. w celach zdrowotnych, związanych z udzielaniem świadczeń zdrowotnych, w tym prowadzeniem i udostępnianiem dokumentacji medycznej - na podstawie art. 9 ust. 2 lit h RODO oraz art. 6 ust. 1 lit. c RODO ;
   b. w celu ochrony przed roszczeniami oraz w celu dochodzenia roszczeń oraz zapewnienia bezpieczeństwa osób i mienia – na podstawie prawnie uzasadnionego interesu Administratora, zgodnie z art. 6 ust. 1 lit. f RODO;
2) Personelu:

WZÓR FIZJOLUX

a. w celu zawarcia oraz realizacji umowy o pracę – na podstawie art. 6 ust. 1 lit. b oraz art. 6 ust. 1 lit. c RODO;

b. w celu profilaktyki zdrowotnej lub medycyny pracy, oceny zdolności do pracy – art. 9 ust. 2 lit. h RODO;

c. w celu zawarcia oraz realizacji umowy cywilnoprawnej - na podstawie art. 6 ust. 1 lit. b oraz art. 6 ust. 1 lit. c RODO;

d. w celu ochrony przed roszczeniami oraz w celu dochodzenia roszczeń, jak również w celu zapewnienia procesu zarządzania przedsiębiorstwem Administratora i zapewnienia bezpieczeństwa osób i mienia – na podstawie prawnie uzasadnionego interesu Administratora, zgodnie z art. 6 ust. 1 lit. f RODO;

e. w celach niewymienionych w lit. a – c – na podstawie zgody osoby, której dane dotyczą, zgodnie z art. 6 ust 1 lit. a RODO;

3) innych osób:

a. w zakresie zawartych umów, w celu zapewnienia ich realizacji – na podstawie art. 6 ust. 1 lit. b RODO;

b. w celu zapewnienia procesu zarządzania przedsiębiorstwem Administratora oraz zapewnienia bezpieczeństwa osób i mienia – na podstawie prawnie uzasadnionego interesu Administratora, zgodnie z art. 6 ust. 1 lit. f RODO;

c. w pozostałych celach - na podstawie zgody osoby, której dane dotyczą, zgodnie z art. 6 ust 1 lit. a RODO, o ile nie zachodzą inne podstawy przetwarzania Danych Osobowych, o których mowa w art. 6 oraz art. 9 RODO.

§ 3.

1. Administrator zapewnia bezpieczeństwo Danych Osobowych w tym ochronę przed ich niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
2. Realizację celów, o których mowa w ust. 1, Administrator zapewnia poprzez:
   a. stosowanie dokumentacji przetwarzania Danych Osobowych, określonej w załącznikach do Polityki;
   b. dopuszczenie do Przetwarzania Danych Osobowych wyłącznie osób upoważnionych przez Administratora na piśmie oraz osób zobowiązanych do zachowania tajemnicy zawodowej w związku z wykonywanym zawodem medycznym (lekarze, pielęgniarki), chyba, że upoważnienie do przetwarzania danych osobowych wynika wprost z przepisów prawa powszechnie obowiązującego;
   c. powierzanie Przetwarzania Danych Osobowych wyłącznie na podstawie odrębnych umów o powierzenie Przetwarzania Danych Osobowych;

WYNOŚCI FIZJOLUX

d. prowadzenie i udostępnianie dokumentacji medycznej zgodnie z przepisami prawa powszechnie obowiązującego w tym m.in. ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (tekst jedn. Dz. U. z 2020 r., poz. 849 ze zm.) oraz rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. 2020, poz. 666);

e. szkolenia Personelu z zakresu zasad Przetwarzania Danych Osobowych;

f. prowadzenie rejestru czynności Przetwarzania, zgodnie z wzorem stanowiącym **załącznik nr 1** do Polityki;

g. monitorowanie naruszeń ochrony Danych Osobowych i prowadzenie rejestru naruszeń, zgodnie z wzorem stanowiącym **załącznik nr 2** do Polityki;

h. stosowanie środków technicznych ochrony Danych Osobowych, w szczególności:

i. ochrony budynku i systemu alarmowego;

ii. zabezpieczeń antywłamaniowych w stolarce drzwiowej i okiennej;

iii. stosowanie szaf i pojemników zapewniających należyty poziom bezpieczeństwa Danych Osobowych;

iv. zabezpieczeń teleinformatycznych (m.in. ograniczony dostęp do systemów, oprogramowanie antywirusowe, firewall, certyfikaty SSL na stronie internetowej).

3. Administrator nie jest zobowiązany do przeprowadzenia oceny skutków dla ochrony Danych Osobowych, o której mowa w art. 35 ust. 1 RODO.

4. Administrator nie jest zobowiązany do wyznaczenia inspektora ochrony danych, o którym mowa w art. 37 ust. 1 RODO.

5. Ogólnodostępne pomieszczenia zakładu leczniczego Administratora są objęte monitoringiem wizyjnym (rejestracja obrazu) w celu zapewnienia bezpieczeństwa Pacjentów oraz Personelu.

6. Dane Osobowe pozyskane w wyniku monitoringu, o którym mowa w ust. 5, Administrator przetwarza wyłącznie dla celów, dla których zostały zebrane, nie dłużej niż 3 miesiące od dnia nagrania, chyba, że nagrania stanowią dowód w postępowaniu prowadzonym na podstawie przepisów ustawy, a organ prowadzący postępowanie wydał stosowne orzeczenie w przedmiocie zabezpieczenia nagrań. W przypadku, o którym mowa w zdaniu poprzedzającym, nagrania przechowywane są przez okres wynikający ze stosownego orzeczenia organu prowadzącego postępowanie lub przez okres trzech miesięcy od zakończenia postępowania.

§ 4.

1. Dostęp Personelu do Danych Osobowych uzasadniony jest zakresem ich zadań i obowiązków oraz wynika z udzielonego upoważnienia do przetwarzania danych osobowych.

2. Personel zobowiązany jest do:

WZÓR BEZPŁATNY

a. zapoznania się z treścią Polityki, a także – w zakresie uzasadnionym zakresem zadań i obowiązków – z przepisami prawa z zakresu ochrony danych osobowych, oraz do bezwarunkowego ich przestrzegania;

b. dbałości o bezpieczeństwo przetwarzanych Danych Osobowych, w tym w szczególności do ich ochrony przed dostępem osób nieuprawnionych, utratą, bezprawną modyfikacją lub zniszczeniem;

c. prowadzenia i udostępniania dokumentacji medycznej Pacjentów zgodnie z obowiązującymi w tym zakresie przepisami prawa oraz jej zabezpieczenia przed utratą lub zniszczeniem;

d. w przypadku udostępniania dokumentacji medycznej – do rzetelnej weryfikacji tożsamości osoby, której dane są udostępniane;

e. w przypadku udostępniania dokumentacji medycznej w formie elektronicznej – do jej uprzedniego zaszyfrowania lub innego zabezpieczenia przed dostępem osób nieuprawnionych;

f. niewynoszenia nośników zawierających Dane Osobowe poza teren zakładu leczniczego Administratora;

g. korzystania z urządzeń oraz systemów teleinformatycznych Administratora w sposób zapewniający ochronę Danych Osobowych przed dostępem osób nieuprawnionych m.in. poprzez:

   i. stosowanie indywidualnych, niepowtarzalnych haseł dostępu,

   ii. niepozostawianie urządzeń bez nadzoru,

   iii. zamykanie pomieszczeń, w których pracują urządzenia, na których przetwarzane są Dane Osobowe,

   iv. wyłączanie urządzeń po zakończeniu użytkowania,

   v. nieudostępniania danych dostępowych (loginów i haseł) osobom nieuprawnionym,

   vi. stosowanie oprogramowania antywirusowego oraz oprogramowania typu *firewall*.

h. zamykania na klucz pomieszczeń, w których przechowywane są Dane Osobowe;

i. przechowywania w miejscu pracy (pokoje, gabinety, recepcja itp.) dokumentów i innych nośników zawierających Dane Osobowe wyłącznie w przeznaczonych do tego pojemnikach/szafach/biurkach;

j. niepozostawiania dokumentów i innych nośników zawierających Dane Osobowe w miejscu pracy w sposób niezabezpieczony przed dostępem osób nieuprawnionych, również po zakończonej pracy („zasada czystego biurka”);

k. nieudostępniania Danych Osobowych osobom, których tożsamości nie można zweryfikować, lub co do której istnieją uzasadnione wątpliwości;

WŁASNOŚĆ FIZJOLUX

l. nieujawniania Danych Osobowych Pacjentów w ogólnodostępnych pomieszczeniach zakładu leczniczego Administratora;

m. niezwłocznego informowania Administratora o każdym przypadku niezgodnego z prawem lub niniejszą Polityką przypadku przetwarzania Danych Osobowych;

n. zachowania poufności Danych Osobowych również po ustaniu stosunku pracy lub innego stosunku prawnego łączącego członka Personelu z Administratorem;

3. Naruszenie postanowień Polityki przez członka Personelu stanowi ciężkie naruszenie obowiązków pracowniczych, a w przypadku osób świadczących na rzecz Administratora pracę na innej podstawie niż stosunek pracy, stanowi rażące naruszenie obowiązków umownych.

§ 5.

1. Administrator może powierzyć Przetwarzanie Danych Osobowych podmiotom trzecim, z których usług korzysta, jeżeli realizacja tych usług wymaga przetwarzania Danych Osobowych, w szczególności:
   a. dostawcom usług hostingowych;
   b. podmiotom serwisującym urządzenia i systemy teleinformatyczne, o ile świadczenie tych usług wiąże się z dostępem do Danych Osobowych;
   c. dostawcom oprogramowania do obsługi informatycznej Administratora, w tym w szczególności oprogramowania do prowadzenia dokumentacji medycznej w formie elektronicznej;
   d. podmiotom świadczącym usługi na rzecz Administratora o ile świadczenie tych usług związane jest z dostępem do Danych Osobowych.
2. Szczegółowe warunki powierzenia Procesorowi przetwarzania Danych Osobowych określa umowa. Wzór umowy powierzenia przetwarzania Danych Osobowych stanowi **załącznik nr 8** do Polityki. Umowa może zostać zawarta w formie pisemnej lub elektronicznej.
3. Administrator może udostępnić Dane Osobowe innym podmiotom wykonującym działalność leczniczą jeżeli jest to uzasadnione procesem leczenia, w szczególności dla zapewnienia ciągłości świadczeń zdrowotnych, oraz innym podmiotom uprawnionym do otrzymania Danych Osobowych na podstawie odrębnych przepisów.

§ 6.

1. Administrator przetwarza Dane Osobowe z poszanowaniem praw osób, których dane dotyczą:
   a. prawa do informacji o Przetwarzaniu Danych Osobowych (art. 13 - 14 RODO);
   b. prawa dostępu do Danych Osobowych oraz uzyskania kopii Danych Osobowych (art. 15 RODO);

WŁASNOŚĆ FIZJOLUX

c. prawa żądania sprostowania Danych Osobowych (art. 16 RODO);

d. prawa żądania usunięcia Danych Osobowych (art. 17 RODO);

e. prawa żądania ograniczenia Przetwarzania Danych Osobowych (art. 18 RODO);

f. prawo przenoszenia Danych Osobowych (art. 20 RODO);

g. prawo sprzeciwu wobec Przetwarzania Danych Osobowych (art. 21 RODO);

h. praw wynikających z przepisów odrębnych.

2. Prawo do informacji jest realizowane przez Administratora poprzez przekazanie osobie, której dane dotyczą, informacji w formie klauzuli informacyjnej. Wzory klauzul informacyjnych stanowią **załączniki nr 6** i **7** do Polityki.

3. Na żądanie osoby, której dane dotyczą, Administrator udostępnia jej kopię Danych Osobowych. Pierwsze udostępnienie następuje nieodpłatnie. Za każde kolejne udostępnienie Administrator pobiera opłatę w wysokości wynikającej z kosztów administracyjnych. O wysokości opłaty Administrator informuje osobę, której dane dotyczą przed udostępnieniem kopii Danych Osobowych.

4. W przypadku, gdy udostępnienie, o którym mowa w ust. 3, dotyczy danych zawartych w dokumentacji medycznej Pacjenta, Administrator udostępnia dokumentację na zasadach określonych w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (tekst jedn. Dz. U. 2020 r., poz. 849 ze zm.). Opłata za każde kolejne udostępnienie dokumentacji medycznej pobierana jest w wysokości określonej w regulaminie organizacyjnym Administratora.

5. W przypadku otrzymania żądania sprostowania Danych Osobowych Administrator niezwłocznie dokonuje weryfikacji zasadności żądania, a w przypadku, gdy żądanie jest uzasadnione – dokonuje sprostowania Danych Osobowych i informuje o tym osobę, której dane dotyczą oraz każdego odbiorcę Danych Osobowych, chyba, że będzie to niemożliwe lub będzie wymagać nadmiernego wysiłku.

6. W przypadku otrzymania żądania usunięcia Danych Osobowych Administrator niezwłocznie dokonuje ich usunięcia, z wyłączeniem przypadków określonych w art. 17 ust. 3 RODO. W odniesieniu do Danych Osobowych zawartych w dokumentacji medycznej Pacjenta usunięcie Danych Osobowych nie może nastąpić przed upływem okresu przechowywania dokumentacji medycznej wynikającego z przepisów prawa powszechnie obowiązującego.

7. Prawo przenoszenia Danych Osobowych oraz prawo sprzeciwu wobec przetwarzania Danych Osobowych nie dotyczą Danych Osobowych przetwarzanych na podstawie art. 9 ust. 2 lit. h RODO.

8. W przypadku otrzymania od osoby, której dane dotyczą, żądania związanego z realizacją praw, o których mowa w ust. 1 lit. b-g, Administrator zobowiązany jest bez zbędnej zwłoki udzielić osobie, której dane dotyczą, udzielić informacji o podjętych działaniach. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od

WERSJA TESTOWA

otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

9. 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.
10. W przypadku odmowy podjęcia działań w związku z żądaniem Administrator informuje osobę, której dane dotyczą o powodach niepodjęcia działań oraz o możliwości złożenia skargi na do Prezesa UODO oraz skorzystania ze środków ochrony prawnej przed sądem.

§ 7.

1. Administrator prowadzi rejestr czynności Przetwarzana Danych Osobowych. Wzór rejestru stanowi **załącznik nr 1** do Polityki.
2. Rejestr czynności Przetwarzania prowadzony jest w formie pisemnej lub elektronicznej i jest udostępniany na każde żądanie Prezesa UODO.

§ 8.

1. Administrator prowadzi rejestr naruszeń ochrony Danych Osobowych. Wzór rejestru stanowi **załącznik nr 2** do Polityki.
2. Naruszeniem ochrony Danych Osobowych jest każde naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych Osobowych, w szczególności:
    a. naruszenie bezpieczeństwa systemów teleinformatycznych wykorzystywanych w działalności Administratora;
    b. udostępnienie Danych Osobom nieuprawnionym lub powstanie bezpośredniego niebezpieczeństwa takiego udostępnienia;
    c. Przetwarzanie Danych Osobowych w sposób sprzeczny z przepisami prawa lub niniejszą Polityką;
    d. bezprawne uszkodzenie, utrata, zmiana lub ujawnienie Danych Osobowych;
    e. naruszenie praw, o których mowa w § 7 ust. 1.
3. W przypadku podejrzenia naruszenia ochrony Danych Osobowych Administrator niezwłocznie weryfikuje, czy doszło do naruszenia i czy naruszenie mogło spowodować ryzyko naruszenia praw i wolności osób, których dane dotyczą.
4. W przypadku stwierdzenia naruszenia, Administrator niezwłocznie, nie później jednak niż w terminie 72 godzin o stwierdzeniu naruszenia zawiadamia Prezesa UODO. Wzór zawiadomienia określa **załącznik nr 3** do Polityki.
5. 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, chyba, że zachodzą okoliczności wskazane w art. 34 ust. 3 RODO.

§ 9.

1. Wszystkie załączniki do Polityki stanowią jej integralną część.
2. Administrator zapoznaje Personel z treścią Polityki i poucza o obowiązku bezwzględnego jej stosowania.

Załączniki:

1) Rejestr czynności przetwarzania;
2) Rejestr naruszeń ochrony danych osobowych;
3) Wzór zgłoszenia naruszeń;
4) Wzór upoważnienia do przetwarzania danych osobowych
5) Wzór ewidencji upoważnień;
6) Wzór klauzuli informacyjnej dla Pacjentów;
7) Wzór klauzuli informacyjnej dla Pracowników;
8) Wzór umowy powierzenia przetwarzania danych osobowych.

WŁASNOŚĆ FIZJOLUX