Polityka Ochrony Danych Osobowych
Fundacji „Saventic”

Spis treści:

§ 1

Postanowienia wstępne

1. Niniejsza polityka ochrony danych osobowych jest dokumentem opisującym sposób przetwarzania danych osobowych oraz obowiązki Fundacji „Saventic”, działającej w charakterze administratora danych osobowych, przetwarzanych w związku z prowadzoną działalnością statutową.
2. Niniejsza polityka poddawana jest bieżącej aktualizacji, nie rzadziej niż raz do roku.
3. Pojęciom stosownym na gruncie niniejszej Polityki nadaje się następujące znaczenie:
    a) **administrator** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

b) **dane dotyczące zdrowia** - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia; do danych o stanie zdrowia należą także informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, takie jak w szczególności: numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych;

c) **dane osobowe (dane)** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;

d) **Inspektor Ochrony Danych (IOD)** - inspektor w rozumieniu art. 37 Rozporządzenia;

e) **naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

f) **odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; nie są odbiorcami organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego;

g) **podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

h) **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;

i) **Rozporządzenie (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;

j) **UODO (Urząd Ochrony Danych Osobowych) -** organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych.

§ 2

Zasady przetwarzania danych osobowych

1. Administrator przetwarza dane osobowe z poszanowaniem poniższych zasad:
   a) legalność - posiada odpowiednią podstawę prawną przetwarzania danych i na niej opiera to przetwarzanie;
   b) rzetelność i prawidłowość - dba o aktualność danych oraz ich poprawność;
   c) przejrzystość - przetwarza dane w sposób przejrzysty dla osoby, której dane dotyczą (w szczególności poprzez informowanie o przetwarzaniu danych);
   d) celowość - przetwarza dane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza danych w sposób niezgodny z tymi celami;
   e) adekwatność - dane są stosowne do celu, w jakim zostały zebrane;
   f) minimalizacja - dane są przetwarzane w zakresie niezbędnym do celu, w jakim zostały pozyskane;
   g) ograniczenie przechowywania - dane przechowywane są przez okres nie dłuższy, niż jest to niezbędne do celów w jakim dane osobowe zostały pozyskane;
   h) integralność i poufność - dba o bezpieczeństwo danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
2. Administrator zapewnia rozliczalność przetwarzania danych osobowych, co oznacza, że jest w stanie wykazać przestrzeganie wszystkich zasad, o których mowa powyżej, w szczególności poprzez stosowanie odpowiednich polityk oraz procedur.

§ 3

Podstawy prawne i generalny zakres przetwarzania danych osobowych

1. Administrator przetwarza dane osobowe:
   a) osób fizycznych, korzystających z pomocy Administratora w zakresie wsparcia ich w procesie diagnostyki chorób rzadkich i chorób ultrarzadkich;
   b) pracowników i osób zatrudnionych w oparciu o umowy cywilnoprawne;
   c) kandydatów do pracy (zatrudnienia);
   d) kontrahentów (osób fizycznych) oraz przedstawicieli kontrahentów (osób fizycznych, działających w imieniu kontrahentów będących podmiotami zbiorowymi);
   e) osób, u których zdiagnozowano chorobę rzadką lub ultrarzadką i które zgodziły się na upublicznienie informacji o ich stanie zdrowia i historii ich choroby, celem zwiększenia świadomości na temat chorób rzadkich i ultrarzadkich.

2. Dane osobowe przetwarzane są:

a) w odniesieniu do osób, o których mowa w ust. 1 lit. a) powyżej:

w zakresie danych osobowych, obejmujących imię i nazwisko, dane kontaktowe, w tym numer telefonu, adres poczty elektronicznej i adres zamieszkania, numer PESEL, wiek i płeć, - na podstawie art. 6 ust. 1 lit. a) RODO, tj. na podstawie dobrowolnej zgody udzielonej przez podmiot danych;

w zakresie danych szczególnych kategorii: dotyczących stanu zdrowia, w szczególność dane dotyczące stanu zdrowia osoby, korzystającej z pomocy Fundacji, opisujące historię diagnostyki i leczenia, oraz danych genetycznych, w zakresie niezbędnym dla zapewnienia pomocy przy diagnozowaniu choroby rzadkiej lub ultrarzadkiej – na podstawie art. 9 ust. 2 lit. a) RODO, tj. na podstawie zgody udzielonej na przetwarzanie danych szczególnych kategorii, udzielonej dobrowolnie przez podmiot danych;

b) w odniesieniu do osób, o których mowa w ust. 1 lit. b) powyżej:

w zakresie danych, których przetwarzanie jest wymagane na gruncie przepisów prawa pracy – na podstawie art. 6 ust. 1 lit. c) RODO, tj. w wykonaniu obowiązków prawnych, ciążących na administratorze;

w zakresie danych identyfikujących stronę umowy i umożliwiających wykonanie tej umowy – na podstawie art. 6 ust. 1 lit. b) RODO, tj. w celu wykonania umowy, której podmiot danych jest stroną;

c) w odniesieniu do osób, o których mowa w ust. 1 lit. c) powyżej:

w zakresie danych podawanych przez kandydata do zatrudnienia na etapie rekrutacji - na podstawie art. 6 ust. 1 lit. a) RODO, tj. na podstawie dobrowolnej zgody, udzielonej przez podmiot danych;

d) w odniesieniu do osób, o których mowa w ust. 1 lit. d) powyżej:

w zakresie danych osobowych strony umowy, niezbędnych do jej wykonania - na podstawie art. 6 ust. 1 lit. b) RODO, tj. w celu wykonania umowy, której podmiot danych jest stroną;

w zakresie danych osobowych reprezentantów stron umowy – na podstawie art. 6 ust. 1 lit. f) RODO, tj. ze względu na prawnie usprawiedliwiony interes Administratora, polegający na zawarciu i wykonywaniu umowy z podmiotem, reprezentowanym jedynie przez osobę fizyczną oraz w celu weryfikacji uprawnienia takiej osoby do zawarcia umowy;

e) w odniesieniu do osób, o których mowa w ust. 1 lit. e) powyżej:

w zakresie danych osobowych, obejmujących imię i nazwisko, dane kontaktowe, w tym numer telefonu, adres poczty elektronicznej i adres zamieszkania, numer PESEL, wiek i płeć, - na podstawie art. 6 ust. 1 lit. a) RODO, tj. na podstawie dobrowolnej zgody udzielonej przez podmiot danych;

w zakresie danych szczególnych kategorii: informacji o stanie zdrowia, w tym w szczególności historii zachorowania na chorobę rzadką lub ultrarzadką – na podstawie

art. 9 ust. 2 lit. a) RODO, tj. na podstawie zgody udzielonej na przetwarzanie danych szczególnych kategorii, udzielonej dobrowolnie przez podmiot danych;

3. Dane osobowe, niebędące danymi szczególnych kategorii mogą być przetwarzane przez Administratora również w celach: marketingowych, promocji usług każdej ze Stron, podejmowania kontaktów z osobą, której dane dotyczą, w tym w celu oferowania jej udziału w realizowanych przez Administratora projektach – na podstawie art. 6 ust. 1 lit. f) RODO, tj. ze względu na prawnie usprawiedliwiony interes Administratora lub na podstawie 6 ust. 1 lit. a) RODO, tj. na podstawie dobrowolnej zgody udzielonej przez podmiot danych.

4. Dane osobowe osób, o których mowa w ust. 1 lit a), d) oraz e) objęte są współadministrowaniem, dokonywanym przez Administratora wraz ze spółką Saventic Health sp. z o.o. Współadministrowanie realizowane jest na podstawie umowy o współpracę, zawartej miedzy Współadministratorami oraz umowy o współadministrowanie danymi osobowymi.

5. Wszelkie zgody na przetwarzanie danych, o których mowa była powyżej, są wyrażane dobrowolnie. Ich niepodanie uniemożliwia jednak korzystanie z usług, oferowanych przez Administratora.

6. Zgody wyrażane są co do zasady w formie pisemnej, natomiast w przypadku przekazywania danych osobowych przez podmioty tych danych za pośrednictwem strony internetowej, zgoda jest udzielana poprzez wypełnienie interaktywnego formularza.

§ 4

Środki organizacyjne i techniczne

1. Administrator stosuje środki techniczne oraz organizacyjne w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu i celu przetwarzania, ryzyka naruszenia praw lub wolności o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. W szczególności administrator stosuje w tym celu:

   a) pseudonimizację oraz szyfrowanie danych;

   b) anonimizowanie wrażliwych danych osobowych po wykorzystaniu ich do prac badawczych przy tworzeniu Algorytmu;

   c) środki zapewniające poufność, integralność, dostępność danych oraz odporność systemów i usług przetwarzania;

   d) środki zapewniające szybkie przywrócenie dostępności danych osobowych i dostęp do nich w razie incydentu fizycznego lub technicznego;

   e) regularne testowanie, mierzenie i ocenę skuteczności tych środków.

2. Administrator prowadzi dokumentację opisującą sposób przetwarzania danych osobowych oraz sposób ich zabezpieczenia, w szczególności w postaci polityk, procedur, wytycznych oraz formularzy.

3. Administrator dopuszcza do przetwarzania danych osobowych jedynie osoby upoważnione przez administratora, które złożyły oświadczenie o zachowaniu danych oraz sposobu ich zabezpieczeń w poufności. Wzór upoważnienia do przetwarzania danych osobowych stanowi **Załącznik** do niniejszej polityki.
4. Administrator prowadzi rejestr osób upoważnionych, którego wzór stanowi **Załącznik** do niniejszej polityki oraz przechowuje treść upoważnień.
5. Administrator wdraża ochronę prywatności na etapie planowania nowych projektów, inwestycji oraz zmian w prowadzonych przez administratora procesach z udziałem danych osobowych.
6. Administrator regularnie szkoli personel posiadający dostęp do danych i podnosi jego wiedzę w zakresie bezpieczeństwa danych osobowych.

§ 5

Rejestr czynności przetwarzania

1. Administrator prowadzi rejestr czynności przetwarzania. Rejestr ten prowadzony jest w formie elektronicznej i stanowi załącznik do niniejszej Polityki.
2. Rejestr czynności przetwarzania administratora zawiera w szczególności:
   a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także przedstawiciela administratora oraz inspektora ochrony danych (jeżeli dotyczy);
   b) określenie celu przetwarzania;
   c) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
   d) opis kategorii odbiorców, który dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach poza Unią Europejską lub w organizacjach międzynarodowych;
   e) jeżeli dane przekazywane są do państw poza Unię Europejską lub do organizacji międzynarodowych - nazwę tego państwa lub organizacji oraz dokumentację odpowiednich zabezpieczeń;
   f) planowane terminy usunięcia poszczególnych kategorii danych (jeżeli możliwe jest ich wskazanie);
   g) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
3. Rejestr czynności przetwarzania jest na bieżąco aktualizowany i udostępniany przez administratora na każde żądanie Urzędu Ochrony Danych Osobowych.

§ 6

Ocena ryzyka

1. Do wyznaczenia poziomu ryzyka dla przetwarzanych danych osobowych Administrator przyjmuje metodę jakościowo-ilościową.
2. Przy wyznaczeniu poziomu prawdopodobieństwa wystąpienia określonego zagrożenia dla danych osobowych przetwarzanych przez Administratora uwzględniono następujące czynniki:
   a) kontekst wewnętrzny i zewnętrzny funkcjonowania,
   b) brak konieczności oceny skutków dla ochrony danych osobowych,
   c) statystyki podobnych zdarzeń w historii,
   d) atrakcyjność podstawowych aktywów (dane osobowe) jak i aktywów wspierających (sprzęt, oprogramowanie, personel, siedziba).
   e) czynniki środowiskowe,
   f) rozwiązania organizacyjne i techniczne,
   g) istniejące zabezpieczenia i podatności urządzeń oraz rozwiązań technicznych,
   h) informacje od użytkowników systemów,
3. Administrator przyjmuje 5 poziomów prawdopodobieństwa wystąpienia zagrożenia dla danych osobowych:
   a) prawie pewne – wartość 5;
   b) prawdopodobne – wartość 4;
   c) możliwe – wartość 3;
   d) mało prawdopodobne – wartość 2;
   e) minimalne – wartość 1.
4. W przypadku skutków wystąpienia zagrożenia dla danych osobowych przetwarzanych w przyjęto 5 poziomów wagi skutku:
   a) bardzo wysoki – wartość 5;
   b) wysoki – wartość 4;
   c) średni – wartość 3;
   d) niski – wartość 2;
   e) bardzo niski – wartość 1.
5. Wyznaczenie poziomu ryzyka dla każdego zbioru danych osobowych polega na wyliczeniu iloczynu prawdopodobieństwa wystąpienia określonego zagrożenia i skutku wystąpienia danego incydentu, według wzoru: R = P x S, gdzie R oznacza poziom ryzyka, P – prawdopodobieństwo wystąpienia zagrożenia, a S – wagę skutku wystąpienia zdarzenia.

6. W celu zobrazowania skutków ryzyka Administrator opracował macierz ryzyka:

PRAWDOPODOBIEŃSTWO			SKUTEK				
			bardzo niski	niski	średni	wysoki	bardzo wysoki
			1	2	3	4	5
	prawie pewne	5	5	10	15	20	25
	prawdopodobne	4	4	8	12	16	20
	możliwe	3	3	6	9	12	15
	mało prawdopodobne	2	2	4	6	8	10
	minimalne	1	1	2	3	4	5

7. W oparciu o macierz ryzyka Administrator określił 4 podstawowe poziomy ryzyka:

   a) bardzo niski (wyniki od 1 do 3): Poziom akceptowalny, nie wymaga podejmowania działań korygujących;

   b) niski (wyniki od 4 do 6): Poziom akceptowalny, decyzja o postepowaniu z ryzykiem należy do Administratora;

   c) średni (wyniki od 7 do 12): Poziom akceptowalny, decyzja o postępowaniu z ryzykiem należy do Administratora;

   d) wysoki (wyniki od 13 do 25): Poziom nieakceptowalny, wymagający podjęcia natychmiastowych działań korygujących.

8. Macierz ryzyka jest stosowana poprzez stosowanie Arkusza oceny ryzyka, którego wzór stanowi Załącznik do niniejszej Polityki. Dokonywanie oceny ryzyka przetwarzania danych osobowych dokumentuje się na piśmie.

9. Decyzja o dalszym postępowaniu z ryzykiem może obejmować cztery rodzaje postepowań:

   a) modyfikowanie (redukcja) ryzyka – polega na obniżeniu poziomu ryzyka (np. poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia) lub zmniejszenie skutków jego wystąpienia. Na przykład zmniejszenie prawdopodobieństwa wystąpienia zdarzenia spowodowanego przerwą w dostawie energii można osiągnąć, włączając w układ zasilania odpowiednią automatykę i niezależne źródła energii (UPS-y, generatory). Zaś zmniejszenie związanych z tym zdarzeniem skutków utraty danych można osiągnąć, modyfikując system wykonywania kopii z wersji, w której kopia wykonywana jest jeden raz na dobę, do postaci, w której kopia jest wykonywana co 15 minut lub w sposób ciągły (na bieżąco) poprzez zastosowanie dodatkowych zabezpieczeń lub modyfikację procedur w sposób pozwalający na zaakceptowanie ryzyka szczątkowego.

b) zachowanie (akceptacja) ryzyka – to świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji (zabezpieczeń), jeżeli poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka.

c) unikanie ryzyka – polega na unikaniu przez ZWIĄZEK działań, które powodują powstanie określonych typów ryzyka, np. w przypadku, gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatny do zysków.

d) przeniesienie ryzyka – polega np. na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta (np. podwykonawcę); należy pamiętać, że przeniesienie ryzyka nie eliminuje go.

10. Analiza ryzyka prowadzona jest co najmniej raz w roku. W przypadku pojawienia się nowych zagrożeń arkusz jest uzupełniany i proces analizy ryzyka rozszerzany o nowe typy zagrożeń dla danych osobowych.

§ 7

Ocena skutków dla ochrony danych

1. Administrator dokonuje oceny skutków dla ochrony danych i dokumentuje fakt dokonania tej oceny.

2. Wykonanie oceny skutków dla ochrony danych jest konieczne, 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 i wolności osób, których dane dotyczą. Dla podobnych operacji przetwarzania wiążących się z podobnym wysokim ryzykiem ocena skutków dla ochrony danych wykonywana jest pojedynczo.

3. Wykonanie oceny skutków dla ochrony danych osobowych wymaga w szczególności:

   a) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie wykorzystującego elementy rozpoznawania cech lub właściwości obiektów znajdujących się w monitorowanej przestrzeni, z użyciem danych osób, których dane dotyczą, prowadzonego przez Fundację, podmiot prowadzący badania kliniczne lub pobierający materiał genetyczny do badań;

   b) przetwarzania na dużą skalę informacji o stanie zdrowia.

4. Administrator monitoruje wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych opublikowany przez Urząd Ochrony Danych Osobowych i dokonuje oceny skutków czynności przetwarzania wskazanych w tym wykazie jako rekomendowanych do poddania tej ocenie.

5. Ocena skutków dla ochrony danych osobowych 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 celu, w jakim dane zostały pozyskane;

c) ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą;

d) środki planowane w celu zmniejszania ryzyka, w tym zabezpieczenia, środki i mechanizmy bezpieczeństwa zapewniające ochronę danych oraz wykazanie przestrzegania przepisów Rozporządzenia.

6. Administrator dokonuje bieżącego przeglądu czynności przetwarzania, celem weryfikacji, czy przetwarzanie to odbywa się w sposób zgodny z dokonaną oceną skutków dla ochrony danych osobowych.

7. Administrator konsultuje się z Urzędem Ochrony Danych Osobowych, jeżeli dokonana ocena skutków dla ochrony danych będzie wskazywała na występowanie wysokiego ryzyka dla praw i wolności osób, których dane dotyczą, jeżeli nie zastosowane zostałyby środki zmniejszające ryzyko. Konsultacje z UODO dokonywane są przed rozpoczęciem przetwarzania danych osobowych.

§ 8

Inspektor ochrony danych

1. Administrator jako podmiot przetwarzający na dużą skalę dane szczególnych kategorii wyznacza wspólnie ze spółką Saventic Health sp. z o.o. inspektora ochrony danych osobowych i dokonał zawiadomienia o wyznaczeniu inspektora do Urzędu Ochrony Danych Osobowych.

2. Inspektor ochrony danych został wyznaczony na podstawie jego kwalifikacji zawodowych, w tym wiedzy oraz zdobytego doświadczenia, które to kwalifikacje zostały udokumentowane.

3. Administrator stwarza inspektorowi ochrony danych odpowiednie warunki, aby mógł realizować swoje obowiązki, w szczególności poprzez:

a) niezwłoczne oraz odpowiedne włączanie go we wszystkie sprawy dotyczące ochrony danych osobowych,

b) zapewnienie zasobów niezbędnych do wykonywania jego zadań oraz utrzymania jego fachowej wiedzy,

c) zapewnienie mu niezależności w sprawowaniu jego funkcji, m.in. poprzez niewydawanie instrukcji dotyczących wykonywania przez niego jego zadań, nieponoszenie przez inspektora negatywnych konsekwencji za wypełnianie przez niego jego zadań, zapewnienie odpowiedniej struktury organizacyjnej aby podlegał jedynie najwyższemu kierownictwu.

4. Zadania inspektora ochrony danych obejmują w szczególności:

a) podnoszenie świadomości wśród personelu przetwarzającego dane osobowe oraz podmiotów przetwarzających dane osobowe na zlecenie administratora, poprzez realizację szkoleń oraz informowanie o obowiązkach spoczywających na tych osobach i podmiotach;

b) monitorowanie przestrzegania przez Administratora przepisów Rozporządzenia i innych przepisów prawa ochrony danych osobowych oraz regulacji wewnętrznych przyjętych u administratora regulujących kwestie związane z przetwarzaniem danych osobowych;

c) wykonywanie audytów w kwestiach związanych z przetwarzaniem danych osobowych;

d) uczestniczenie oraz wspieranie administratora w dokonywaniu oceny skutków dla ochrony danych oraz monitorowanie wykonania oceny tych skutków;

e) współpraca z Urzędem Ochrony Danych Osobowych;

f) sprawowanie funkcji punktu kontaktowego dla osób, których dane dotyczą w kwestiach związanych z przetwarzaniem danych osobowych.

§ 9

Powierzenie przetwarzania danych osobowych

1. Administrator może korzystać z usług podmiotów zewnętrznych w celu wspierania administratora w jego bieżącej działalności, w szczególności polegających na dostarczeniu oraz/lub utrzymaniu infrastruktury teleinformatycznej, w tym narzędzi wspierających administratora w prowadzeniu dokumentacji medycznej w formie elektronicznej.
2. Administrator korzysta wyłącznie z usług takich dostawców usług, którzy zapewniają odpowiednie gwarancje bezpieczeństwa danych osobowych i zgodności przetwarzania danych z przepisami Rozporządzenia.
3. Administrator dokonuje weryfikacji podmiotu przetwarzającego przed dokonaniem wyboru takiego podmiotu, jak również dokonuje jego późniejszej, okresowej weryfikacji, zgodnie z przyjętą u administratora procedurą, weryfikacja jest dokumentowana.
4. Administrator zawiera z podmiotem przetwarzającym umowę powierzenia przetwarzania danych osobowych lub reguluje okoliczność powierzenia przetwarzania danych innym instrumentem prawnym, w której określone zostają obowiązki podmiotu przetwarzającego wynikające z faktu powierzenia. Wzór umowy powierzenia przetwarzania danych osobowych stanowi Załącznik do niniejszej Polityki.
5. Administrator nie przekazuje danych osobowych do państw poza terenem Unii Europejskiej.

§ 10

Obowiązki personelu

1. Dostęp do danych osobowych posiada niezbędny personel Administratora.
2. Personel administratora zobowiązany jest do:

   a) zapoznania się oraz stosowania przepisów prawa w zakresie ochrony danych osobowych, w tym Rozporządzenia;

b) ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem do tych danych, ich nieuzasadnioną modyfikacją lub zniszczeniem;

c) niszczenia w bezpieczny sposób wszelkich nośników zawierających dane osobowe (w formie papierowej jak i elektronicznej);

d) korzystania z zasobów informatycznych oraz sprzętu w sposób zgodny z ich przeznaczeniem i w sposób bezpieczny, m.in. poprzez okresową zmianę haseł, zachowanie poufności loginów i haseł oraz niepozostawianie sprzętu bez nadzoru;

e) niezwłocznego informowania przełożonych o zaobserwowanych nieprawidłowościach, które mogą mieć wpływ na bezpieczeństwo przetwarzanych danych osobowych;

f) przechowywania dokumentacji zawierającej dane osobowe w przeznaczonych do tego miejscach, z ograniczonym dostępem osób trzecich, zwłaszcza dokumentacji medycznej;

3. Personel ponosi odpowiedzialność za należyte wykonywanie swoich obowiązków i jest on pouczony przez Administratora o sankcjach wynikających z nieprawidłowości w tym zakresie, w tym o odpowiedzialności karnej.

§ 11

Prawa osób, których dane dotyczą

1. Administrator przetwarza dane osobowe z poszanowaniem praw osób, których dane dotyczą wynikających z RODO.
2. Administrator prowadzi rejestr zgłoszonych żądań, przez osoby, których danych dotyczą.
3. Przed wykonaniem praw osoby, której dane dotyczą administrator dokonuje weryfikacji tożsamości osoby zgłaszającej żądanie, celem ustalenia, czy żądanie pochodzi od osoby uprawnionej.
4. Administrator zapewnia odpowiednie zaplecze techniczne oraz kadrowe w celu terminowej oraz rzetelnej realizacji praw osoby, której dane dotyczą. Zgłoszone żądania realizowane są przez administratora niezwłocznie, nie później niż w terminie miesiąca od otrzymania żądania. W przypadku niemożności wykonania żądania w w/w terminie, z uwagi na skomplikowany charakter sprawy, administrator kontaktuje się z osobą, której dane dotyczą i informuje ją o przyczynie wydłużenia tego terminu oraz przewidywanym terminie realizacji żądania osoby, której dane dotyczą.

§ 12

Prawo do informacji

1. Osoby, których dane dotyczą, są informowane przez administratora o sposobie przetwarzania ich danych osobowych oraz przysługującym ich uprawnieniach w formie klauzuli informacyjnej, z którą mogą zapoznać się w każdej chwili w siedzibie administratora, jego jednostkach organizacyjnych oraz na stronie internetowej.

2. Klauzula informacyjna jest wydawana w czasie wyrażania zgody na przetwarzanie danych osobowych.

3. Klauzula informacyjna jest sporządzona prostym językiem, w sposób przejrzysty i wyczerpuje wszystkie informacje zgodnie z art. 13 oraz 14 RODO.

§ 13

Prawo dostępu do danych

1. Na żądanie osoby, której dane dotyczą, administrator udziela jej informacji o sposobie przetwarzania jego danych osobowych. Na żądanie osoby, której dane dotyczą, administrator udostępnia mu nieodpłatnie pierwszą kopię jego danych osobowych; za każdą kolejną kopię administrator może pobrać opłatę w rozsądnej wysokości.

3. Jeżeli żądanie wydania kopii danych zostało złożone administratorowi w formie elektronicznej a osoba, której dane dotyczą nie zaznacza inaczej - kopia wydawana jest w tej samej formie.

4. Administrator może udostępnić kopię w inny sposób, niż wybrany przez osobę, której dane dotyczą, jeżeli ze względów technicznych nie jest to możliwe (np. ze względu na wagę pliku w wersji elektronicznej); o niemożności dostarczenia kopii w wybrany przez osobę, której dane dotyczą, sposób oraz proponowanym alternatywnym rozwiązaniu administrator niezwłocznie powiadamia tę osobę.

§ 14

Prawo do sprostowania danych

1. Administrator umożliwia osobie, której dane dotyczą, niezwłoczne sprostowanie jego danych osobowych, jeżeli są one nieprawidłowe lub nieaktualne, lub ich uzupełnienie.

2. Administrator może żądać od osoby, której dane dotyczą, stosownych dokumentów w celu okazania, aby ustalić zasadność oraz zgodność z prawem dokonywanej zmiany danych osobowych.

§ 15

Prawo do usunięcia, ograniczenia i przenoszenia danych

1. Administrator usuwa bez zbędnej zwłoki dane osobowe osoby, której dane dotyczą, na jej żądanie, jeżeli na administratorze nie spoczywają obowiązki nakazujące dalsze przetwarzanie danych osobowych.

2. Odmowa realizacji prawa do usunięcia danych jest przekazywana przez administratora osobie, której dane dotyczą, wraz z uzasadnieniem przyczyny odmowy zawierającym podstawy prawne odmowy.

3. Na żądanie osoby, której dane dotyczą, administrator dokonuje ograniczenia przetwarzania jej danych osobowych.

4. Na żądanie osoby administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora.

§ 16

Prawo do sprzeciwu

Jeżeli osoba, której dane dotyczą zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po jego stronie ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, albo zaistnieją podstawy do ustalenia, dochodzenia lub obrony roszczeń.

§ 17

Naruszenia ochrony danych osobowych

1. Administrator stosuje procedury postępowania w przypadku naruszeń lub podejrzeń naruszeń ochrony danych osobowych.

2. Administrator prowadzi rejestr naruszeń ochrony danych osobowych oraz dokumentuje wszystkie okoliczności związane z naruszeniami. Wzór rejestru naruszeń stanowi Załącznik do niniejszej Polityki.

3. W przypadku naruszeń ochrony danych osobowych mogących skutkować naruszeniem praw lub wolności osoby, której dane dotyczą, administrator dokonuje zgłoszenia takiego naruszenia Urzędowi Ochrony Danych Osobowych w terminie 72 godzin od stwierdzenia naruszenia.

4. W celu dotrzymania terminu, o którym mowa w pkt 7.1.3. administrator wprowadza do umowy powierzenia przetwarzania danych lub innego instrumentu regulującego kwestię powierzenia przetwarzania danych, odpowiednie postanowienia zobowiązujące podmiot przetwarzający do niezwłocznego zgłaszania administratorowi wszelkich naruszeń ochrony danych osobowych oraz udzielania wszelkich okoliczności dotyczących tych naruszeń.

5. W przypadku, jeżeli naruszenie skutkowałoby wysokim ryzykiem naruszenia praw i wolności osoby, której dane dotyczą, administrator bez zbędnej zwłoki zawiadamia również tę osobę i informuje ją jasnym i prostym językiem o okolicznościach naruszenia oraz podjętych środkach mających na celu zapobieżenie jego negatywnym skutkom.

§ 18

Udostępnianie danych osobowych

Administrator udostępnia dane osobowe podmiotom trzecim, z którymi zawarł umowy o współpracę i które z mocy obowiązujących przepisów są niezależnymi administratorami danych osobowych.

§ 19

Pozostałe dokumenty

1. Administrator opracowuje i wdraża szczególne dokumenty, zapewniające transparentność i bezpieczeństwo przetwarzania danych osobowych.
2. Załącznikami do niniejszej Polityki są:
   a) wzór arkuszu oceny ryzyka,
   b) rejestr czynności przetwarzania,
   c) rejestr upoważnień do przetwarzania danych osobowych,
   d) wzór upoważnienia do przetwarzania danych osobowych
   e) rejestr naruszeń ochrony danych osobowych,
   f) wzór umowy powierzenia przetwarzania danych osobowych,
   g) wzór ogólnej zgody na przetwarzanie danych osobowych oraz klauzuli informacyjnej,
   h) wzór zgody na przetwarzanie danych medycznych dla podopiecznych Administratora oraz przeznaczona dla nich klauzula informacyjna,
   i) wzór zgody na przetwarzanie danych medycznych dla podopiecznych Administratora oraz przeznaczona dla nich klauzula informacyjna, wyrażanej za pośrednictwem strony internetowej,
   j) wzór zgody na przetwarzanie danych medycznych dla osób, które chorowały na chorobę rzadką lub ultrarzadką oraz przeznaczona dla nich klauzula informacyjna,
   k) wzór upoważnienia do dostępu do dokumentacji medycznej i do informacji o stanie zdrowia,
   l) opis technicznych i organizacyjnych środków zabezpieczeń.
3. Administrator stosuje zabezpieczenia techniczne i organizacyjne danych osobowych w sposób opisany w Opisie technicznych i organizacyjnych środków zabezpieczeń, stanowiącym załącznik do niniejszej Polityki.