POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W POLSKIM STOWARZYSZENIU TERAPEUTÓW TERAPII SKONCENTROWANEJ NA ROZWIĄZANIACH

WARSZAWA 2021

Spis treści

I. Informacje ogólne

1. Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Polskiego Stowarzyszenia Terapeutów Terapii Skoncentrowanej na Rozwiązaniach jako Administratora Danych Osobowych z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.

2. Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

- ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2019.1781 t.j.) ;

- rozporządzeniu 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 [rozporządzenie ogólne o ochronie danych].

3.Wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne. Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania. Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. Należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe. Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu (motyw 39 RODO).

4. Aby przetwarzanie było zgodne z prawem, powinno się odbywać na podstawie zgody osoby, której dane dotyczą, lub na innej uzasadnionej podstawie przewidzianej prawem, w tym musi się odbywać

z poszanowaniem obowiązku prawnego, któremu podlega administrator, lub z poszanowaniem umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (motyw 40 RODO).

5. Zgoda powinna być wyrażona w drodze jednoznacznej potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego lub ustnego oświadczenia (motyw 32 RODO).
Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania. Zgodnie z dyrektywą Rady 93/13/EWG ([1]) oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiała i łatwo dostępną formę, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków. Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych. Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji (motyw 42 RODO).

6. Przetwarzanie powinno być zgodne z prawem, jeżeli jest ono niezbędne w związku z zawarciem umowy lub zamiarem zawarcia umowy (motyw 44 RODO).

7. Jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę przetwarzania powinno stanowić prawo Unii lub prawo państwa członkowskiego (motyw 45 RODO).

8. Zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych (motyw 60 RODO).

9. Informacje o przetwarzaniu danych osobowych dotyczących osoby, której dane dotyczą, należy przekazać tej osobie w momencie zbierania danych, a jeżeli danych nie uzyskuje się od osoby, której dane dotyczą, lecz z innego źródła – w rozsądnym terminie, zależnie od okoliczności (motyw 61 RODO).

10. Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem (motyw 63 RODO).

11. Każda osoba fizyczna powinna mieć prawo do sprostowania danych osobowych jej dotyczących oraz prawo do „bycia zapomnianym”, jeżeli zatrzymywanie takich danych narusza rozporządzenie RODO, prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator. Osoba, której dane dotyczą, powinna w szczególności mieć prawo do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli dane te nie są już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane, jeżeli osoba, której dane dotyczą, cofnęła zgodę lub jeżeli wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących, lub jeżeli przetwarzanie jej danych osobowych nie jest z innego powodu zgodne z rozporządzeniem RODO (motyw 65 RODO).

12. Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów rozporządzenia RODO. Aby móc wykazać przestrzeganie rozporządzenia RODO, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych.

13. Obszarem przetwarzania danych osobowych przez Polskie Stowarzyszenie Terapeutów Terapii Skoncentrowanej na Rozwiązaniach jest siedziba Stowarzyszenia przy ulicy Patriotów 44A/9, 04-912 Warszawa.

14. Ochrona danych osobowych realizowana jest poprzez stosowanie zabezpieczeń w postaci środków organizacyjnych, środków ochrony fizycznej oraz środków technicznych systemu informatycznego w ramach procedur zawartych w Polityce Bezpieczeństwa Danych Osobowych.

15. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Polskim Stowarzyszeniu Terapeutów Terapii Skoncentrowanej na Rozwiązaniach rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.

16. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów:

1) **Poufność danych** – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;

2) **Integralność danych**– zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

3) **Dostępność informacji** – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;

4) **Rozliczalność danych** – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

5) **Autentyczność danych** – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;

6) **Integralność systemu** – nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;

7) **Zarządzanie ryzykiem** – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych;

8) **Minimalizacja danych –** przetwarzanie danych stosownych, ograniczonych, niezbędnych i adekwatnych do realizacji celów w których zostały zebrane.

17. Administrator Danych Osobowych gromadzi i przetwarza dane osobowe w celu realizacji zadań statutowych w stosunku do członków Stowarzyszenia.

II. Definicje

1. Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1)Polityka Bezpieczeństwa – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w Polskim Stowarzyszeniu Terapeutów Terapii Skoncentrowanej na Rozwiązaniach;

2)Administrator Danych Osobowych– Administratorem Danych Osobowych w rozumieniu niniejszej Polityki Bezpieczeństwa jest Polskie Stowarzyszenie Terapeutów Terapii Skoncentrowanej na Rozwiązaniach, które zgodnie z § 27 Statutu Stowarzyszenia reprezentowane jest przez Prezesa Zarządu i Członka Zarządu lub dwóch Członków Zarządu działających łącznie;

3)Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

4)Przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

5) Ograniczenie przetwarzania – oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

6) Profilowanie - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

7) Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są

objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

8) Zbiór danych -oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

9) Administrator - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

10) Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.;

11) Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

12) Strona trzecia - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

13) Zgoda - osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

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

15) Szczególne kategorie danych osobowych:

- „dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

- „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub

behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

- „dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

16) Organizacja międzynarodowa - oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;

17)Biuro – Biuro Polskiego Stowarzyszenia Terapeutów Terapii Skoncentrowanej na Rozwiązaniach;

18) Ustawa -Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2019.1781 t.j.);

19)RODO - Rozporządzeniu 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 [rozporządzenie ogólne o ochronie danych];

20)Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą;

21)System informatyczny - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

22) Bezpieczeństwo systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnionym przetwarzaniem danych;

23)Administrator Systemu Informatycznego – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych;

15) Użytkownik - rozumie się przez to osobę wyznaczoną i upoważnioną przez Administratora danych do przetwarzania danych osobowych, przeszkoloną w zakresie ochrony tych danych;

16) Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

III. Cel i zakres Polityki

1. Ustawa o ochronie danych osobowych nakłada na Administratora Danych obowiązek stosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz zabezpieczenie ich między innymi przed udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy, a także zmianą, utratą, uszkodzeniem lub zniszczeniem. Celem niniejszej Polityki Bezpieczeństwa przetwarzania danych osobowych jest opracowanie optymalnych i zgodnych z wymogami prawa zasad przetwarzania danych, których zbieranie i przetwarzanie jest niezbędne dla realizacji zadań statutowych Polskiego Stowarzyszenia Terapeutów Terapii Skoncentrowanej na Rozwiązaniach oraz dla bieżącej działalności Stowarzyszenia.

2. W Polskim Stowarzyszeniu Terapeutów Terapii Skoncentrowanej na Rozwiązaniach przetwarzane są przede wszystkim dane osobowe członków Stowarzyszenia oraz osób współpracujących ze Stowarzyszeniem na podstawie umów cywilnoprawnych. Stowarzyszenie, w związku z realizacją zadań statutowych, przetwarza także dane osobowe beneficjentów i wnioskodawców, a także dane uczestników szkoleń organizowanych przez Stowarzyszenie. Wykaz poszczególnych zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych w Polskim Stowarzyszeniu Terapeutów Terapii Skoncentrowanej na Rozwiązaniach stanowi załącznik nr 2 do Polityki Bezpieczeństwa.

3. Dane osobowe we wskazanych powyżej zbiorach danych są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.

4. Politykę Bezpieczeństwa stosuje się przede wszystkim do:

1) wszystkich informacji dotyczących danych osób współpracujących ze Stowarzyszeniem na podstawie umów cywilnoprawnych, w tym danych osobowych i treści zawieranych umów;

2) wszystkich danych dotyczących członków Polskiego Stowarzyszenia Terapeutów Terapii Skoncentrowanej na Rozwiązaniach oraz innych osób, które wypełniły deklarację członkowską Stowarzyszenia;

3) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;

4) rejestru osób dopuszczonych do przetwarzania danych osobowych;

5) innych dokumentów zawierających dane osobowe.

5. Zakres ochrony danych osobowych określony w Polityce Bezpieczeństwa ma zastosowanie do systemów informatycznych Polskiego Stowarzyszenia Terapeutów Terapii Skoncentrowanej na Rozwiązaniach, w których są przetwarzane dane osobowe, a w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;

2) wszystkich lokalizacji - pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

3) wszystkich osób świadczących pracę bądź usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie do przetwarzania danych osobowych.

6. Do stosowania zasad określonych w Polityce Bezpieczeństwa zobowiązani są wszyscy Użytkownicy danych, w tym w szczególnościzleceniobiorcy oraz wszelkie inne osoby mające dostęp do informacji podlegających ochronie, w tym zwłaszcza członkowie organów Polskiego Stowarzyszenia Terapeutów Terapii Skoncentrowanej na Rozwiązaniach.

IV. Obowiązki i odpowiedzialność

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych (art. 24 RODO).

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślne 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 (art. 25 RODO).

1. Do najważniejszych obowiązków Administratora Danych należy:

1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO oraz innych przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych;

2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa;

3) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;

4) przeprowadzanie szkoleń użytkowników przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe;

5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

6) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;

7) nadzór nad bezpieczeństwem danych osobowych;

8) kontrola działań użytkowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;

9) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;

10) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;

11) optymalizacja wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego;

12) instalacja i konfiguracja oprogramowania systemowego, sieciowego, oprogramowania służącego do zarządzania bazą danych;

13) konfiguracja i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem;

14) współpraca z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych;

15) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego;

16) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;

17) zmiana lub usprawnienie procedur bezpieczeństwa i standardów zabezpieczeń;

18) zarządzanie licencjami oraz procedurami ich dotyczącymi;

19) prowadzenie profilaktyki antywirusowej.

2. Do najważniejszych obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

1) znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej;

2) przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami;

3) postępowanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;

4) zachowanie w tajemnicy danych osobowych, do których uzyskały dostęp oraz informacji o sposobach ich zabezpieczenia;

5) ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;

6) informowanie Administratora Danych Osobowych o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe;

7) zapoznanie się z Polityką Bezpieczeństwa przetwarzania danych osobowych.

V. Zarządzanie ochroną danych osobowych

1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.

2. Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.

3. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.

4. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.

5. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

6. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.

7. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

8. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 29 RODO. Upoważnienia wydawane są indywidualnie przez Administratora Danych Osobowych.

VI. Szkolenia użytkowników

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych.

3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz Polityką Bezpieczeństwa Danych obowiązującymi w Polskim Stowarzyszeniu Terapeutów Terapii Skoncentrowanej na Rozwiązaniach. Po zaznajomieniu się z powyższymi regulacjami, użytkownik, przed dopuszczeniem do przetwarzania danych, powinien zobowiązać się do ich przestrzegania przez podpisanie oświadczenia użytkownika, stanowiącego załącznik nr 4 do Polityki Bezpieczeństwa.

VII. Upoważnienie do przetwarzania danych osobowych

1. Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 29 RODO.

2. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych.

3. W celu otrzymania przez Użytkownika upoważnienia do przetwarzania danych osobowych, należy dostarczyć do Administratora Danych podpisane oświadczenie użytkownika.

4. Na podstawie otrzymanego oświadczenia Administrator Danych Osobowych upoważnia Użytkownika do przetwarzania danych osobowych i wydaje upoważnienie do przetwarzania danych osobowych sporządzane wg wzoru stanowiącego załącznik nr 4 i 5 do Polityki Bezpieczeństwa. Upoważnienia,
o których mowa powyżej przechowywane są w Biurze.

5. Upoważnienie może być w każdym czasie odwołane przez Administratora Danych Osobowych. Oświadczenie o odwołaniu upoważnienia do przetwarzania danych osobowych powinno być sporządzone na piśmie. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą ustania przesłanki będącej podstawą wydania upoważnienia, ustania członkostwa w Stowarzyszeniu lub w organie Stowarzyszenia, jeżeli nadanie upoważnienia związane było ze sprawowaniem funkcji w organie Stowarzyszenia.

VIII. Ewidencja osób upoważnionych

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Polskim Stowarzyszeniu Terapeutów Terapii Skoncentrowanej na Rozwiązaniach jest prowadzona przez Administratora Danych zgodnie ze wzorem formularza stanowiącym załącznik nr 3 do Polityki Bezpieczeństwa przetwarzania danych osobowych w Stowarzyszeniu.

IX. Powierzenie danych osobowych

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 RODO 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, która wiąże podmiot przetwarzający i administratora, określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Wzór umowy powierzenia danych osobowych stanowi załącznik nr 11 do niniejszej Polityki Bezpieczeństwa Przetwarzania Danych Osobowych. Umowa stanowi w szczególności, że podmiot przetwarzający:

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora;

b) zapewnia by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

c) podejmuje wszelkie środki wymagane na mocy art. 32 RODO;

d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w 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;

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO;

g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym dziale oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora do przeprowadzenia audytów, w tym inspekcji i przyczynia się do nich.

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 te same obowiązki ochrony danych jak w umowie między administratorem a podmiotem przetwarzającym, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO. 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 pierwszym podmiocie przetwarzającym.

X. Dokonanie obowiązku informacyjnego

1.Administrator danych osobowych zgodnie z wymogami wynikającymi z artykułu 12, 13 oraz 14 rozporządzenia wywiązuje się z obowiązku informacyjnego wobec osób których dane dotyczą poprzez:

a) opublikowanie informacji wymaganych w artykule 13 oraz 14 na tablicach ogłoszeń oraz przy wejściu do strefy przetwarzania;

b) opublikowanie informacji wymaganych w artykule 13 oraz 14 na stronie internetowej administratora danych;

c) informowanie o przetwarzaniu danych osobowych przed rozpoczęciem ich przetwarzania wobec każdej osoby fizycznej indywidualnie.

2. Informacje o których mowa powyżej mają charakter zwięzły, pisany jasnym i prostym językiem zgodnie z wymogami artykułu 12 rozporządzenia.

3. 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;

b) cele przetwarzania danych osobowych oraz podstawę prawna przetwarzania;

c) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;

d) informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

e) okres, przez który dane osobowe będą przechowywane;

f) 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;

g) 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;

h) informacje o prawie wniesienia skargi do organu nadzorczego;

i) informacje, 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;

j) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

4. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, następujące informacje:

a) swoją tożsamość i dane kontaktowe;

b) cele przetwarzania, do których maja posłużyć dane osobowe, oraz podstawę prawna przetwarzania;

c) kategorie odnośnych danych osobowych;

d) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;

e) informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

f) okres, przez który dane osobowe będą przechowywane;

g) 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;

h) 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;

i) informacje o prawie wniesienia skargi do organu nadzorczego;

j) źródło pochodzenia danych osobowych;

k) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

XI. Przetwarzanie danych osobowych. Wymagania bezpieczeństwa.

1. Dane osobowe mogą być przetwarzane wyłącznie w obszarze przetwarzania danych osobowych, na które składają się pomieszczenia biurowe w siedzibie Polskiego Stowarzyszenia Terapeutów Terapii Skoncentrowanej na Rozwiązaniach, z wyjątkiem sytuacji udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych. Szczegółowy wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych znajduje się w załączniku nr 6 do Polityki Bezpieczeństwa.

2. Dane osobowe w Polskim Stowarzyszeniu Terapeutów Terapii Skoncentrowanej na Rozwiązaniach przetwarzane są przy zastosowaniu zabezpieczeń zapewniających ich ochronę w postaci środków organizacyjnych, technicznych i środków ochrony fizycznej.

3. Zgodnie z treścią rozporządzenia administrator w celu ochrony danych osobowych zapewnia następujące organizacyjne środki ochrony danych:

a) każda osoba będąca pracownikiem Administratora przetwarzająca dane osobowe zostaje do tego pisemnie upoważniona przez Administratora;

b) Administrator wydaje upoważnienie do przetwarzania na podstawie wzoru upoważnienia do przetwarzania danych;

c) użytkownik po uzyskaniu upoważnienia podpisuje oświadczenie zgodnie ze wzorem oświadczenia osoby upoważnionej o zachowaniu poufności;

d) Administrator prowadzi Rejestr upoważnień do Przetwarzania, w którym zawarte są informacje wskazujące zakres zbiorów oraz zakres czynności przetwarzania realizowanych przez upoważnioną osobę;

e) upoważnieni użytkownicy wpisani do Rejestru Upoważnień objęci są cyklicznymi szkoleniami z zakresu Ochrony Danych Osobowych;

f) Administrator powierzając przetwarzanie danych zewnętrznemu podmiotowi przetwarzającemu, niebędącemu pracownikiem Administratora, powierza przetwarzanie na podstawie wzoru umowy o powierzenie przetwarzania danych;

g) Administrator prowadzi Rejestr umów powierzenia przetwarzania.

4. Zgodnie z treścią rozporządzenia administrator w celu ochrony danych osobowych zapewnia następujące fizyczne środki ochrony danych:

a) dokumenty zawierające dane osobowe poza godzinami pracy osób upoważnionych do przetwarzania danych zamykane są na klucz w szafkach w pomieszczeniach przetwarzania;

b) pomieszczenia przetwarzania danych podczas nieobecności osób upoważnionych do przetwarzania danych a także poza godzinami pracy tych osób, zamykane są na klucz, a klucze przechowywane są w pomieszczeniu dozorowanym;

c) drzwi zwykłe (niewzmacniane, nie przeciwpożarowe) do pomieszczeń, w których przetwarzane są dane osobowe znajdują się wewnątrz budynku w strefie ograniczonego dostępu;

d) zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie;

e) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek.

5. Zgodnie z treścią rozporządzenia administrator w celu ochrony danych osobowych zapewnia następujące teleinformatyczne środki ochrony danych:

a) dane osobowe przetwarzane w systemach teleinformatycznych sporządzane i przechowywane są w formie dokumentów elektronicznych pod kontrola systemu operacyjnego posiadającego wsparcie producenta, w kontekście użytkownika systemu posiadającego indywidualny login oraz hasło;

b) zbiory danych osobowych przetwarzane są wyłącznie na autoryzowanym sprzęcie służbowym;

c) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

XII. Sprawdzenie stanu systemu ochrony danych osobowych

1. Administrator Bezpieczeństwa Informacji raz w roku sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

2. Okresowy przegląd Polityki Bezpieczeństwa powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Stowarzyszenia oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

XIII. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych

1. Każdy użytkownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym poinformować Administratora Danych.

2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;

2) niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;

3) nieprzestrzeganie zasad ochrony danych osobowych przez członków Stowarzyszenia.

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:

1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);

2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych);

3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych prowadzi postępowanie wyjaśniające w toku którego:

1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;

2) inicjuje ewentualne działania dyscyplinarne;

3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;

4) dokumentuje prowadzone postępowania.

5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:

1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;

2) zabezpiecza ewentualne dowody;

3) ustala osoby odpowiedzialne za naruszenie;

4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);

5) inicjuje działania dyscyplinarne;

6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;

7) dokumentuje prowadzone postępowania zgodnie ze wzorem Raportu z naruszenia bezpieczeństwa danych osobowych stanowiących załącznik nr 10do Polityki Bezpieczeństwa.

XIV. Zgodność

Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Polskiego Stowarzyszenia Terapeutów Terapii Skoncentrowanej na Rozwiązaniach, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

XV. Postanowienia końcowe

1. Administrator Danych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.

2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.

4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.