POLITYKA

OCHRONY DANYCH OSOBOWYCH

w Fundacji Rozwój i Zdrowie

ul. Potulickich 34, 05-510 Konstancin - Jeziorna

Wstęp

Niniejsza „Polityka Ochrony Danych Osobowych” jest dokumentem opisującym zasady ochrony danych osobowych stosowane w Fundacji Rozwój i Zdrowie z siedzibą w Konstancinie - Jeziorna, przy ul. Potulickich 34 (05-510)**.** Dokument zawiera wytyczne postępowania z danymi osobowymi w ramach podmiotu w oparciu o przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. **w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy z 10 maja 2018 r. o ochronie danych osobowych.**

Polityka Ochrony Danych Osobowych jest podstawowym dokumentem systemu ochrony danych osobowych, przetwarzanych w podmiocie, biorąc pod uwagę stosowanie zasad.

Przetwarzanie odbywa się:

1) w oparciu o podstawę prawną i zgodnie z prawem;
2) rzetelnie i uczciwie;
3) w sposób przejrzysty dla osoby, której dane dotyczą;
4) w konkretnych celach i nie „na zapas”;
5) w zakresie w jakim jest to konieczne;
6) z dbałością o prawidłowość danych;
7) nie dłużej niż jest to wymagane, bądź istnieje taka potrzeba;
8) zapewniając odpowiednie bezpieczeństwo danych.

Podstawą prawną przetwarzania danych osobowych beneficjentów, darczyńców, klientów oraz pracowników i usługodawców są bezpośrednio właściwe przepisy RODO pozostające w związku z przepisami prawa pracy i innymi przepisami prawa.

ROZDZIAŁ I: Terminy i definicje użyte w dokumencie „Polityka Ochrony Danych Osobowych”

„Prezes Urzędu Ochrony Danych Osobowych” - organ właściwy do spraw ochrony danych osobowych na terytorium Polski, utworzony ustawą z 10 maja 2018 roku o ochronie danych osobowych. Jest również organem nadzorczym w rozumieniu ogólnego rozporządzenia o ochronie danych (RODO).

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

„RODO” - rozporządzenie ogólne Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r w sprawie ochrony danych osobowych osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016r (Dz. Urz. UE L 119 z 04-05-2016r).

„Dane osobowe” - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak: nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego tożsamości tej osoby fizycznej.

„Dane wrażliwe” - to dane szczególnie chronione (sensytywne) informujące o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, przynależności partyjnej lub związkowej, jak również dane o stanie zdrowia, kodzie genetycznym, danych biometrycznych, nałogach lub życiu seksualnym a także dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

„Przetwarzanie danych osobowych” - to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje :

- Zbieranie, rejestrowanie, organizowanie,
- Strukturyzowanie, przechowywanie, adaptację lub zmianę,
- Wyszukiwanie, konsultacje, wykorzystanie,
- Ujawnianie poprzez transmisję, rozpowszechnianie,
- Udostępnianie w inny sposób, wyrównanie lub połączenie,
- Ograniczenie, usunięcie lub zniszczenie danych osobowych

„Ograniczenie przetwarzania” - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

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

„Zgoda osoby, której dane dotyczą” - oznacza dobrowolne, dowolnie określone, konkretne, świadome i jednoznaczne wyrażenie zgody, wskazanie osoby, której dane dotyczą za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie jej danych osobowych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić. Zgoda nie może tez być domniemana lub dorozumiana. Powinna być wyrażona jasnym i prostym językiem.

„Poufność danych” - właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym podmiotom.

„Integralność” - właściwość zapewniająca, że dane osobowe nie zostały zmienione, zniszczone w sposób nieautoryzowany.

„Rozliczalność” - oznacza, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

„Ocena skutków w ochronie danych” - to proces przeprowadzany przez Administratora jeśli jest wymagany przez obowiązujące prawo, jeśli to konieczne, z uczestnictwem Inspektora Ochrony Danych, przed przetwarzaniem w przypadku wystąpienia wysokiego ryzyka dla praw i wolności osób fizycznych. Należy uwzględnić wykorzystanie nowych technologii przy

przetwarzaniu danych osobowych uwzględniając charakter, zakres, kontekst i cel przetwarzania oraz ryzyko. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

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

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

„Podmiot przetwarzający” - (procesor) – to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu Administratora.

„Inspektor Ochrony Danych (IOD)” - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/procesorowi, a także pracownikom i usługodawcom w zakresie obowiązującego prawa o ochronie danych osobowych i niniejszej „Polityki Ochrony Danych Osobowych” oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób, których dane dotyczą, są przetwarzane jak i organu nadzorczego – Urzędu Ochrony Danych Osobowych.

„Pseudonimizacja” - oznacza przetwarzanie danych osobowych w taki sposób (np. zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonej osoby bez użycia dodatkowych informacji, narzędzi lub urządzeń.

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

„Naruszenie ochrony danych osobowych” - jest to przypadkowy lub celowy niezgodny z prawem incydent prowadzący do: zniszczenia, utracenia, zmodyfikowania, nieuprawnionego dostępu, nieuprawnionego ujawnienia danych osobowych osoby fizycznej.

ROZDZIAŁ II: Osoby odpowiedzialne za ochronę danych osobowych

Administratorem danych osobowych jest Fundacja Zdrowie i Rozwój, a w jej imieniu funkcję tą sprawuje Prezes Fundacji, który zobowiązał wszystkie osoby wykonujące pracę na rzecz Administratora, (które uzyskały upoważnienia do przetwarzania danych osobowych wymienione w **załączniku nr 1** do niniejszego dokumentu) do dostosowania ich postępowania do wymogów wynikających z Polityki Ochrony Danych Osobowych.

Administrator dokonuje kontroli zabezpieczenia danych, przestrzegania obowiązujących zasad, procedur, instrukcji i klauzul przez usługodawców oraz usługodawców i zatrudnionych pracowników we własnym zakresie. W razie potrzeby Administrator może powołać Inspektora Danych Osobowych (IOD). Szczegółowe zadania, obowiązki, uprawnienia i odpowiedzialność (IOD), w razie jego powołania zawiera **załącznik nr 2** niniejszej „Polityki Ochrony Danych Osobowych".

ROZDZIAŁ III: Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych

Ogólne zasady i postanowienia bezpieczeństwa przetwarzania danych w Fundacji Zdrowie i Rozwój są następujące:

1) Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik lub usługodawca mający dostęp do danych;
2) Pracownicy oraz usługodawcy mający dostęp do danych osobowych w ramach udzielonego upoważnienia nie mogą ich ujawniać zarówno w miejscu pracy jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych;
3) W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej, pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka", co oznacza, że nie pozostawia się materiałów zawierających dane osobowe umożliwiając dostęp do nich osobom nieupoważnionym. Za realizację i przestrzeganie tej zasady odpowiedzialny jest każdy pracownik na swym stanowisku pracy;

4) Niszczenie brudnopisów, niepotrzebnych kopii dokumentów zawierających dane musi odbywać się w sposób uniemożliwiający odczytanie treści np. za pomocą niszczarek;
5) Zabronione jest wynoszenie materiałów zawierających dane poza obszar ich przetwarzania bez ważnego związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony;

6) Osoby nieuprawnione mogą przebywać w pomieszczeniach w których przetwarzane są dane osobowe tylko w obecności osoby upoważnionej do przetwarzania danych osobowych;
7) Wszyscy pracownicy oraz usługodawcy zobowiązani są do zamykania na klucz wszelkich pomieszczeń i budynków wchodzących w skład obszarów, w których przetwarzane są dane zarówno w czasie ich chwilowej nieobecności jak i po zakończeniu dnia pracy. Klucze nie mogą być pozostawione w zamkach drzwi. Osoby posiadające klucze zobowiązane są do dołożenia należytej staranności odnośnie bezpiecznego ich przechowywania.

Pozostałe zasady ochrony danych osobowych obowiązujące w podmiocie:

1) Dane osobowe, a w szczególności imiona i nazwiska, numery PESEL, serie i numery dowodów osobistych, numery telefonów, zdjęcia osób, nagrania z monitoringu i wszelkie inne dane pozwalające zidentyfikować osobę fizyczną muszą być chronione przed dostępem osób nieupoważnionych.
2) Zabrania się zapisywać dane osobowe w inny sposób lub w innej formie, niż to wynika z zakresu obowiązków na zajmowanym stanowisku.
3) Zabrania się pobierania od osób fizycznych dokumentów tożsamości takich jak, dowód osobisty, prawo jazdy, paszport lub jakichkolwiek innych urzędowych dokumentów osobistych. Dokumenty te mogą być przedstawione jedynie do wglądu celem sporządzenia adnotacji, a właściciel dokumentu tożsamości nie może tracić go z oczu.
4) Zabrania się udostępniania osobom nieupoważnionym danych osobowych, a w szczególności faktur, umów, korespondencji, danych biznesowych, zamówień oraz wszelkich innych nośników zawierających dane osobowe.

5) Zabrania się pozostawiania bez nadzoru osób upoważnionych nośników danych osobowych pendrive, dyskietek, dysków twardych komputerowych w publicznie dostępnych miejscach takich jak sale konferencyjne, pokoje spotkań, oraz w innych dostępnych miejscach, do których może mieć dostęp osoba nieupoważniona.
6) Zabrania się ujawniania w miejscach publicznych danych osobowych poprzez rozmowy (w tym telefoniczne), wezwania głosowe lub inne formy werbalnego ujawniania danych osobowych identyfikujących osoby fizyczne.
7) Należy w sposób szczególny chronić tzw. dane wrażliwe (sensytywne), takie jak : informacje o stanie zdrowia, nałogach, życiu seksualnym, dane genetyczne, dane biometryczne, wyroki skazujące, skazania i orzeczenia sądowe lub kary administracyjne, mandaty karne i kwestionariusze osobowe – CV.
8) W przypadku kradzieży lub podejrzenia ujawnienia danych osobowych osobie nieupoważnionej, należy niezwłocznie powiadomić bezpośredniego przełożonego oraz Administratora lub IOD.
9) Wszelkie dane osobowe przetwarzane w podmiocie stanowią własność Fundacji ale muszą być udostępniane osobom fizycznym na każde ich wezwanie czy prośbę.
10) Nieprzestrzeganie powyższych obowiązków może być potraktowane przez pracodawcę jako ciężkie naruszenie postanowień umownych. Może spowodować i prowadzić do natychmiastowego rozwiązania umowy o pracę. Za poniesione straty Administrator może dochodzić rekompensaty na drodze sądowej, a także złożyć zawiadomienie do organów ścigania o popełnienie czynu zabronionego narażającego prawa i wolności osób fizycznych.
11) Pracownik lub usługodawca, który widział incydent lub naruszenie ma obowiązek w trybie natychmiastowym poinformować Administratora lub IOD najpóźniej w ciągu 24 godzin, gdyż Administrator ma obowiązek poinformować o incydencie organ nadzorczy w terminie 72 godzin. Zgodnie z przepisami pracownik lub usługodawca ma obowiązek podjąć stosowne działania przewidziane procedurami i instrukcjami dotyczącymi ochrony danych osobowych.

W przypadku naruszenia ochrony danych:

1) Ogólny tryb postępowania i zachowania się pracowników oraz usługodawców w przypadku wystąpienia naruszenia zasad ochrony danych osobowych reguluje art. 33 RODO, który mówi, że w przypadku naruszenia ochrony danych Administrator bez

zbędnej zwłoki nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je organowi nadzorczemu wg. właściwości, zadań i uprawnień o czym stanowi art. 55 – RODO;

2) Administrator dokumentuje wszelkie naruszenia ochrony danych, w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na zweryfikowanie przestrzegania przepisów (art. 33 i 34 RODO).

Istotę naruszenia ochrony danych osobowych, szczegółowe w tym zakresie postępowanie oraz sankcje karne zawiera **załącznik nr 5** do niniejszego dokumentu.

ROZDZIAŁ IV: Wykaz zbiorów danych osobowych przetwarzanych przez Fundację Zdrowie i Rozwój:

Administrator danych przetwarza dane osobowe w następujących zbiorach danych:

1. Zbiór I. „Kandydaci na Podopiecznych oraz Podopieczni" - Zbiór stanowią dane osób, które są Kandydatami oraz Podopiecznymi Fundacji, obejmują: imię i nazwisko Kandydata oraz Podopiecznego Fundacji, a także uczestnika szkolenia, seminarium, warsztatów, datę urodzenia Kandydata oraz Podopiecznego, adres do korespondencji, telefon, e-mail.
    a) Dane są pozyskiwane bezpośrednio od osób, których dane dotyczą lub od osób pośredniczących i przetwarzane są w postaci papierowej (w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych) lub przy pomocy systemu informatycznego.
    b) Dane zbioru udostępniane są Zarządowi oraz pracownikom i usługodawcom w niezbędnym zakresie.
    c) Dane osobowe pozyskiwane są bezpośrednio od osób, których dane dotycz,. natomiast przetwarzane są na podstawie przepisów prawa oraz wyrażonej zgody np. przelewanie wynagrodzenia na wskazany rachunek bankowy.
    d) Dane ze zbioru są udostępniane członkom Zarządu i komisji rewizyjnej (jeśli została powołana) w celu realizacji zadań statutowych, jak również są udostępniane bankowi, w którym Fundacja posiada rachunek bankowy, ZUS, urzędowi skarbowemu oraz innym osobom lub organom, w wypadkach prawem

przewidzianych lub na podstawie pisemnej umowy o powierzenie przetwarzania danych osobowych (nazwy i adresy instytucji do wglądu).

e) Dane osobowe w tym zbiorze przetwarzane są w formie papierowej lub przy pomocy systemu informatycznego.

2. Zbiór II. „PERSONEL ” - Zbiór obejmuje dane pracowników oraz usługodawców (obecnych i byłych). Zawiera niezbędne dane (np. dla celów naliczania podatków oraz na poczet ubezpieczeń społecznych).
    a) Dane osobowe pozyskiwane są bezpośrednio od osób, których dane dotycz,. natomiast przetwarzane są na podstawie przepisów prawa oraz wyrażonej zgody np. przelewanie wynagrodzenia na wskazany rachunek bankowy.
    b) Dane ze zbioru są udostępniane członkom Zarządu i komisji rewizyjnej (jeśli została powołana) w celu realizacji zadań statutowych, jak również są udostępniane bankowi, w którym Fundacja posiada rachunek bankowy, ZUS, urzędowi skarbowemu oraz innym osobom lub organom, w wypadkach prawem przewidzianych lub na podstawie pisemnej umowy o powierzenie przetwarzania danych osobowych (nazwy i adresy instytucji do wglądu).
    c) Dane osobowe w tym zbiorze przetwarzane są w formie papierowej lub przy pomocy systemu informatycznego.
3. Zbiór III. „REKRUTACJA PERSONELU” - Zbiór stanowią dane osobowe, osób ubiegających się o zatrudnienie lub współpracę w ramach umów cywilnych. Dane zbierane są od osób, których te dane dotyczą. Przetwarzanie danych dokonuje się drogą internetową z wykorzystaniem poczty elektronicznej lub w wersji papierowej.

Fundacja Zdrowie i Rozwój przetwarza dane osobowe kandydatów do pracy oraz dane osobowe pracowników i usługodawców w zakresie w jakim zezwala na to treść art. 22 (1) Kodeksu pracy i tylko w celach związanych z zatrudnieniem. Podmiot nie wykorzystuje ich w innych celach, aniżeli te wskazane w zdaniu poprzednim. Dane te pozyskiwane są bezpośrednio do kandydatów do pracy, bądź od podmiotów zajmujących się profesjonalnie pośrednictwem pracy, o ile przedsiębiorcy ci przetwarzają dane osobowe kandydatów w sposób zgodny z przepisami prawa.

Dane osobowe, których przetwarzanie nie znajduje uzasadnienia w świetle powyższego przepisu przetwarzane są wyłącznie na podstawie zgody osoby, której dane dotyczą – zgoda może być wyrażona w dowolnej formie.

Powyższe zapisy dotyczą także osób zatrudnianych na podstawie umów cywilnoprawnych.

Dane osobowe kandydatów do pracy przetwarzane są wyłącznie przez czas trwania i w celu rekrutacji danego kandydata do pracy. W przypadku, gdy kandydat wyrazi odrębną zgodę na przetwarzania jego danych osobowych na potrzeby przyszłych rekrutacji, jego oferta przechowywana jest przez okres 1 roku. Po tym czasie dane danego kandydata podlegają zniszczeniu.

Na podstawie zawartej umowy powierzenia przetwarzania danych osobowych, dane pracowników oraz usługodawców mogą zostać przekazane do podmiotu specjalizującego się w prowadzeniu księgowości i obsługi kadrowej, tj. przedsiębiorcy wykonującego na rzecz podmiotu usługi prowadzenia księgowości oraz zajmującego się rozliczaniem i odprowadzaniem składek na ubezpieczenie społeczne oraz zdrowotne pracowników, usługodawców oraz współpracowników Fundacji Zdrowie i Rozwój. Akta osobowe pracowników oraz usługodawców mogą być przechowywane w siedzibie podmiotu, z którym zawarto umowę powierzenia przetwarzania danych. W takiej sytuacji, Administrator, będzie posiadał kopie tych dokumentów w postaci elektronicznej.

Fundacja nie gromadzi danych osobowych z wykorzystaniem systemów informatycznych. W przypadku rozpoczęcia gromadzenia danych osobowych z wykorzystaniem systemów informatycznych Fundacja wprowadzi Instrukcję zarządzania systemem informatycznym (wzór Instrukcji znajduje się w **załączniku nr 3** do niniejszego dokumentu).

ROZDZIAŁ V: Opis struktury zbiorów danych i sposobu przepływu danych pomiędzy poszczególnymi systemami w formie rejestru czynności przetwarzania

1. Na opis struktury zbiorów danych składa się nazwa, opis danego zbioru wraz z podaniem aktywów i tryb procesu przetwarzania z opisem funkcjonalnym. Każdy opis zbioru zawiera w sobie następujące parametry:
    - Nazwa zbioru – opis kategorii osób,
    - Cele przetwarzania,
    - Kategorie odbiorców,
    - Kategorie odbiorców w państwach trzecich,

- Planowane terminy usunięcia poszczególnych kategorii danych,
- Opis technicznych i organizacyjnych środków bezpieczeństwa,
- Opis kategorii danych osobowych,
- Podstawa prawna przetwarzania.

2. W opisie procesu przetwarzania zawarte są te informacje, które odnoszą się w swej treści do charakterystyki danego zbioru, zatem są dla każdego zbioru inne i się różnią.

ROZDZIAŁ VI: Analiza ryzyka

1. Analiza ryzyka to procedura opisująca sposób w jaki przeprowadzono analizę ryzyka w celu zabezpieczenia danych osobowych, adekwatnie do zidentyfikowanych najczęściej występujących zagrożeń wynikających przede wszystkim z:
   - Utraty danych,
   - Modyfikacji danych osobowych,
   - Nieuprawnionego ujawnienia,
   - Nieuprawnionego dostępu do danych,
   - Nieuprawniony dostęp do danych podczas przechowywania,
   - Niezgodnego z prawem zniszczenia.

2. Analiza ryzyka przeprowadzona została dla w/w zagrożeń określonych zbiorów związanych z procesem przetwarzania.

3. REJESTR CZYNNOŚCI PRZETWARZANIA - Administrator zgodnie z art. 30 RODO jest zobowiązany do prowadzenia rejestru czynności przetwarzania. Rejestr ten stanowi podstawę do przeprowadzenia analizy ryzyka. Administrator prowadzi rejestr opisany w **załączniku nr 6.**

4. WYZNACZENIE ZAGROŻEŃ:

   1) Administrator odpowiada za określenie listy zagrożeń, naruszenia poufności, dostępności i integralności, które mogą wystąpić podczas przetwarzania danych;
   2) Zagrożenia są identyfikowane w odniesieniu do uprzednio zinwentaryzowanych zbiorów (kategorii osób), aktywów oraz procesów przetwarzania z opisem funkcjonalnym;
   3) Zagrożenia jakie mogą wystąpić w Fundacji to:
      - Nieuprawnione ujawnienie danych osobowych,
      - Nieuprawniony dostęp do danych podczas przesyłania,
      - Nieuprawniony dostęp do danych podczas przechowywania,
      - Przypadkowe lub niezgodne z prawem zniszczenie lub uszkodzenie danych,
      - Przypadkowe lub niezgodne z prawem utracenie danych osobowych,
      - Przypadkowe lub niezgodne z prawem zmodyfikowanie danych osobowych.

5. WYZNACZENIE RYZYKA DLA ZAGROŻEŃ - Wyznaczenie ryzyka dla zagrożeń, dokonuje się w jednostce z zastosowaniem następującej formuły obliczeniowej:

R = P * S

Gdzie:

R - oznacza ryzyko wystąpienia incydentu a przypisana mu skala wynosi (od 1 do 9).

P - oznacza prawdopodobieństwo wystąpienia incydentu a przypisana mu skala wynosi (od 1 do 3).

S - oznacza skutki wystąpienia incydentu a przypisana mu skala wynosi (od 1 do 3).

Gdzie :

Wartość 1 - oznacza prawdopodobieństwo, skutek, ryzyko **małe.**

Wartość 2 - oznacza prawdopodobieństwo, skutek, ryzyko **średnie.**

Wartość 3 - oznacza prawdopodobieństwo, skutek, ryzyko **wysokie.**

6. Interpretacja uzyskanych wyników oznacza, że w przypadku uzyskania wyniku w granicach (od 1 do 4) **ryzyko jest akceptowalne** i nie wymaga dodatkowych zabezpieczeń.
7. W przypadku uzyskania wyniku oceny zagrożenia w granicach (od 5 do 6) to oznacza, że ryzyko jest **opcjonalne akceptowalne/nieakceptowalne.** Do decyzji Administratora pozostawia się podjęcie decyzji, którą ocenę wybierze. W przypadku wyboru oceny nieakceptowalnej, Administrator stosuje dodatkowe zabezpieczenia i środki adekwatne do celu i wyznacza osoby odpowiedzialne za realizację zadania.
8. Natomiast uzyskanie oceny ryzyka dla zagrożeń o skali w granicach (od 7 do 9) oznacza, że ryzyko jest **nieakceptowalne** i wymaga od Administratora podjęcia natychmiastowych i koniecznych środków zaradczych, programu naprawczego. Administrator decyduje o zastosowaniu dodatkowych środków bezpieczeństwa i wyznacza osoby odpowiedzialne za realizację zadania, lub wdraża odpowiedni dostosowany do zagrożenia program naprawczy.

ROZDZIAŁ VII: Upoważnienia

Upoważnienie do przetwarzania danych osobowych to **kluczowy element** systemu ochrony danych osobowych w podmiocie. Upoważnienie do przetwarzania danych to dokument, w którym Administrator nadaje upoważnienia dla poszczególnych osób uprawniający go do pracy z danymi osobowymi.

W przypadku powzięcia informacji, bądź zaistnienia uzasadnionego przypuszczenia, że dana osoba upoważniona nie zachowuje w poufności treści przetwarzanych danych osobowych bądź poprzez swoje zachowanie naraża na utratę bądź zagraża integralności danych Administrator niezwłocznie blokuje dostęp tej osobie do zbioru danych.

Zasady nadawania uprawnień są następujące:

1) Gromadzone dane osobowe są udostępniane osobom zatrudnionym przez Fundację oraz usługodawcom w zakresie minimalnym, niezbędnym do wykonywania ich pracy na danych stanowisku lub związanym z charakterem podejmowanych obowiązków na danym stanowisku lub w związku z innymi zleconymi zadaniami i zawsze w oparciu o posiadane upoważnienie do przetwarzania danych osobowych;

2) Pracownicy oraz usługodawcy otrzymują upoważnienia do konkretnych zbiorów danych i tylko w tych zbiorach mogą przetwarzać dane;

3) Powierzenie danych osobowych odbywa się na podstawie:

   - wzoru upoważnienia zatwierdzonego przez Fundację,

   - klauzuli w umowie głównej, z zastrzeżeniem uwzględnienia wszystkich wymagań zawartych we wzorze upoważnienia.

4) W uzasadnionych przypadkach dopuszczalne jest podpisanie umowy powierzenia na wzorze kontrahenta, z zastrzeżeniem, że musi on gwarantować zabezpieczenie interesu Fundacji, a także realizację praw osób, których dane dotyczą

5) Upoważnienie nadane pracownikowi oraz usługodawcy ma w swoim założeniu minimalizować ryzyko wycieku danych osobowych. Podpisując taki dokument, pracownik oraz usługodawca będzie bardziej świadomy ciążącej na nim odpowiedzialności;

6) Nadanie upoważnienia zobowiązuje każdego pracownika oraz usługodawcę do zapoznania się z przepisami i regulacjami wewnętrznymi z zakresu ochrony danych osobowych;
7) Nadanie upoważnienia jest ściśle powiązane z ewentualnym wystąpieniem incydentu, gdy konieczne będzie ustalenie czy dany pracownik, bądź usługodawca działał w ramach nadanego mu uprawnienia;
8) Nadanie uprawnienia może w wielu sytuacjach (o ile takowe by wystąpiły) zwolnić całkowicie lub częściowo z odpowiedzialności Administratora w związku z wystąpieniem incydentu czy naruszenia;
9) Nadawanie upoważnień może być zsynchronizowane z nadawaniem uprawnień w systemie informatycznym (jeśli dotyczy);
10) W upoważnieniu wskazane powinno być do jakich konkretnie systemów informatycznych ma dostęp dany pracownik lub usługodawca organizacji (jeśli dotyczy).
11) Administrator jest zobowiązany do prowadzenia rejestru incydentów bezpieczeństwa i korzystania z prawa udostepnienia danych, który stanowi **załącznik nr 4.**
12) Poza w/w informacją w treści upoważnienia do przetwarzania danych osobowych, obowiązkowo znajdują się następujące informacje:

a) Podstawa prawna i kto nadaje upoważnienie,
b) Forma upoważnienia,
c) Forma zapoznania się z zasadami ochrony danych,
d) Kto decyduje i ponosi odpowiedzialność za nadanie upoważnienia,
e) Kto ewidencjonuje nadane upoważnienia.

ROZDZIAŁ VIII: Środki techniczne i organizacyjne zabezpieczające dane osobowe

W celu stworzenia właściwych zabezpieczeń, organizacyjnych i technicznych w podmiocie wprowadzone się następujące środki organizacyjne:

1) Ochrona pomieszczeń wykorzystanych do przetwarzania danych osobowych:

a) Siedziba Fundacji znajduje się przy ul. Potulickich 34, 05-510 Konstancin – Jeziorna,
b) Administrator danych osobowych przetwarza dane osobowe w swojej siedzibie wskazanej w ust. a),
c) Obszar przetwarzania danych osobowych obejmuje zamykane na klucz pomieszczenie - siedzibę Fundacji,
d) Dokumentacja papierowa po godzinach pracy przechowywana jest w zamykanych biurkach i szafach podmiotu,
e) Przebywanie osób nieuprawnionych w obszarze przetwarzania danych jest dopuszczalne tylko w obecności osób upoważnionych do przetwarzania.

2) Przedsięwzięcia w zakresie zabezpieczenia sprzętu komputerowego:

a) Dla zapewnienia ciągłości działania systemów informatycznych służących do przetwarzania danych osobowych, stosuje się w nich sprzęt wraz z oprogramowaniem wyprodukowane przez renomowanych producentów z licencjonowanym oprogramowaniem wraz z zabezpieczeniem przed awarią zasilania czy zakłóceniami w sieci zasilającej;
b) Zbiory danych osobowych oraz programy służące do przetwarzania są chronione i zabezpieczone przed nieuprawnionym dostępem i opisane są w „Instrukcji zarządzania systemem informatycznym”;

c) Kopie danych tworzy i za nie odpowiada Administrator. Kopie zapasowe całego serwera robione są codziennie, na bieżąco oraz w sposób automatyczny.

3) Przedsięwzięcia w zakresie ochrony teletransmisji danych:

W celu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z Internetu stosowane są zabezpieczenia chroniące przed nieuprawnionym dostępem poprzez zabezpieczenie zasobów informatycznych oprogramowaniem antywirusowym. Oprogramowanie antywirusowe jest automatyczne i na bieżąco aktualizowane.

4) Przedsięwzięcia w zakresie środków ochrony w ramach oprogramowania systemów:

W celu zapewnienia kontroli operacji dokonywanych przez użytkowników systemu informatycznego, w systemie dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło. Hasło dostępu do systemu operacyjnego lub aplikacji składa się z co najmniej 8 znaków, zawiera małe i wielkie litery, oraz cyfry i znaki specjalne.

5) Przedsięwzięcia w zakresie środków ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

a) W celu ochrony zbiorów danych osobowych prowadzonych w systemach informatycznych przed nieuprawnionym dostępem, stosuje się mechanizmy kontroli dostępu do tych danych.

b) Nośniki danych, zawierające dane osobowe są przechowywane w miejscach uniemożliwiających dostęp do nich osobom nieupoważnionym.

c) Po ustaniu przydatności danych osobowych zawartych na nośnikach, dane są trwale usuwane (bez możliwości odtworzenia ich treści).

d) Urządzenia, dyski, pendrive lub inne nośniki informacji zawierające dane osobowe nie nadające się do naprawy, są niszczone w sposób uniemożliwiający odczytanie zapisanych na nich informacji.

6) Przedsięwzięcia w zakresie środków ochrony w ramach systemu użytkowego:

a) W celu ochrony danych osobowych przetwarzanych na stacjach roboczych na czas krótkotrwałego opuszczenia stanowiska pracy przez użytkownika systemu, stosuje się mechanizm blokady stacji roboczej – wygaszacz ekranu zabezpieczony hasłem.

b) Przed opuszczeniem miejsca pracy na dłuższy czas, użytkownik obowiązany jest wylogować się z systemu lub zablokować komputer.

c) Całkowicie zabronione jest instalowanie nieautoryzowanych programów na stacjach roboczych.

7) Przedsięwzięcia w zakresie środków organizacyjnych:

a) W przypadku uznania za niezbędne, Fundacja w celu przestrzegania procedur, zasad, klauzul zgodnie z RODO wprowadzi „Instrukcję zarządzania systemem informatycznym".

b) Na bieżąco monitorowane są przez Administratora wdrożone zabezpieczenia i rozwiązania służące ochronie i bezpieczeństwa przetwarzanych danych osobowych.
c) Co najmniej raz do roku przeprowadzane są przeglądy i uaktualnienia najważniejszych dokumentów dotyczących ochrony i bezpieczeństwa danych jak „Polityka Ochrony Danych Osobowych" i inne,
d) Cały personel zobowiązany został do zachowania w tajemnicy sposobów i metod przetwarzania danych osobowych oraz zastosowanych środków ochrony i bezpieczeństwa zarówno w czasie trwania zatrudnienia jak i po jego ustaniu.
e) Każda osoba przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych zostaje zaznajomiona z aktualnymi przepisami w zakresie ochrony danych

osobowych oraz z dokumentami w postaci Polityki Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym (jeśli dotyczy).

f) W razie potrzeby osoby dopuszczone do pracy przy przetwarzaniu danych osobowych podlegają okresowym szkoleniom obejmującymi zagadnienia związane z ochroną danych osobowych.

ROZDZIAŁ IX: Obszar w którym przetwarzane są dane osobowe

Obszar pomieszczeń, w których przetwarzane są dane osobowe obejmuje zarówno miejsca, w których wykonuje się operacje na danych (wpisuje, modyfikuje, kopiuje) jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe, w tym w szczególności w siedzibie Fundacji przy ul. Potulickich, 05-510 Konstancin - Jeziorna.

ROZDZIAŁ X: Postanowienia końcowe

Treść „Polityki Ochrony Danych Osobowych" jest dokumentem wewnętrznym Fundacji Zdrowie i Rozwój i nie może być udostępniana w żadnej formie osobom nieuprawnionym.

Każda osoba zatrudniona w Fundacji przetwarzająca dane osobowe, zobowiązana jest do zapoznania się z treścią tego dokumentu jak i z „Instrukcją Zarządzania Systemem Informatycznym" (jeśli dotyczy).

Wszyscy usługodawcy oraz pracownicy zatrudnieni w podmiocie, zobowiązani są do bezwzględnego przestrzegania przy przetwarzaniu danych osobowych wszystkich **postanowień, zasad RODO i nowej ustawy o ochronie danych osobowych, instrukcji, procedur i klauzul.** Dokumenty takie jak „Polityka Ochrony Danych Osobowych", „Instrukcja Zarządzania Systemem Informatycznym" (jeśli dotyczy) są najważniejszymi dokumentami systemu ochrony danych osobowych jaki funkcjonuje w Fundacji Zdrowie i Rozwój.