**Polityka Ochrony Danych Osobowych**

**Klinika Rehabilitacji Sportowej ORTOREH A. Piotrowski, E. Witek-Piotrowska sp.j**

# Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora – Klinikę Rehabilitacji Sportowej ORTOREH w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi środek organizacyjny, mający na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

DEFINICJE

**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 parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)

**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. tożsamość tej osoby fizycznej.

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

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

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

**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 przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

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

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

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

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

# Ocena skutków (analiza ryzyka)

Ocena skutków jest formalną, procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator.

## Opis operacji przetwarzania (inwentaryzacja aktywów)

1. W celu dokonania analizy dokonano zidentyfikowania danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w załączniku nr 1 Wykaz zbiorów danych osobowych.
2. Opis zbiorów powinien obejmuje takie informacje, jak:
	1. nazwę zbioru (opis kategorii osób)
	2. opis celów przetwarzania
	3. charakter, zakres, kontekst danych osobowych
	4. odbiorcy danych
	5. opis operacji przetwarzania

## Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator przetwarzający dane osobowe spełnia wobec nich obowiązki prawnych. W szczególności zapewnia, że :

1. dane te są legalnie przetwarzane,
2. dane te są adekwatne w stosunku do celów przetwarzania,
3. dane te są przetwarzane przez określony czas,
4. wobec tych osób wykonano tzw. obowiązek informacyjny wraz ze wskazaniem ich praw w tym: prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody.
5. opracowano i zebrano podpisy pod klauzulami informacyjnymi dla powyższych osób zgodnie z treścią załącznika nr 2 .
6. podpisano umowy powierzenia z podmiotami przetwarzającymi (przykład postanowień umowy przetwarzania określa załącznik nr 3). Umowy są rejestrowane w załączniku nr 4 Rejestr umów powierzenia.

## Analiza ryzyka

Dokonano analizy ryzyka i określono listę zagrożeń, które mogą wystąpić w przetwarzaniu danych. Wykaz przykładowych zagrożeń znajduje się w załączniku nr 5 Lista potencjalnych zagrożeń.

# Regulamin Ochrony Danych Osobowych

Stworzono regulamin ochrony danych osobowych, stanowi on załącznik nr 6 Regulamin Ochrony Danych Osobowych.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania potwierdzenie stanowi załącznik nr 7 - Oświadczenie poufności.