POLITYKA BEZPIECZEŃSTWA INFORMACJI

CAALM CLINIC Sp. z o.o.

Ul. Piastowska 4, 42-600 Tarnowskie Góry

REGON: 527300197

	Wersja nr 2	Obowiązuje od dnia: 04.11.2024 r.	
	Imię i nazwisko	**Data**	**Podpis**
Zatwierdził Administrator Danych	Andrzej Grabowski	31.10.2024 r.	

Dokumenty powiązane:

Instrukcja zarządzania systemem informatycznym

Spis treści:

§ 1

Wprowadzenie

1. Polityka Bezpieczeństwa Informacji w dalszej części dokumentu zwana Polityką opracowana została w oparciu o następujące przepisy prawa:

    a) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO)

2. Polityka bezpieczeństwa rozumiana jest jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Instytucji. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

3. Celem Polityki jest wdrożenie i realizacja działań przy wykorzystaniu środków technicznych i organizacyjnych, które zapewnią maksymalny poziom bezpieczeństwa w zakresie przetwarzania danych osobowych, chroniąc je przed nieautoryzowanym dostępem, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

4. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
*poufności – właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
*integralności – właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
*rozliczalności – właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
*zgodności z prawem – właściwości zapewniającej, że gromadzone są wyłącznie dane niezbędne do właściwego funkcjonowania przedsiębiorstwa.

5. Polityka zakłada pełne zaangażowanie kierownictwa oraz wszystkich pracowników Caalm Clinic dla zapewnienia bezpieczeństwa danych osobowych przetwarzanych zarówno w sposób tradycyjny papierowy, jak i w systemach informatycznych.

6. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawa oraz w związku ze zmianami, które powodują, że określone zasady przestają być aktualne.

§ 2

Definicje

Administrator Danych (AD) – Caalm Clinic Sp. z o.o. , ul. Piastowska 4 42-600 Tarnowskie Góry; NIP: 6452584681 ; REGON: 527300197, decydująca o celach i środkach przetwarzania danych osobowych

Inspektor danych osobowych (IDO) – osoba wyznaczona przez Administratora na podstawie Art. 37 ust.1 rozporządzenia, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych

Administrator Systemów Informatycznych (ASI) - podmiot wyznaczony przez Administratora Danych na podstawie umowy na obsługę informatyczną

Dane osobowe – każda informacja dotycząca osoby fizycznej, która w sposób pośredni lub bezpośredni pozwala ją zidentyfikować, w szczególności poprzez podanie jednego lub kilku specyficznych czynników ją określających

Dane szczególnych kategorii - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

PUODO – Prezes Urzędu Ochrony Danych Osobowych

Naruszenie ochrony danych osobowych – zamierzone lub przypadkowe działanie lub zaniechanie działania, powodujące zagrożenie bezpieczeństwa danych osobowych, przetwarzanych tradycyjnie, jak również z wykorzystaniem systemów informatycznych

Osoba upoważniona – osoba posiadająca imienne upoważnienie wydane przez Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji dopuszczona jako użytkownik do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu

Strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe

Osoba trzecia - należy przez to rozumieć, osobę nie będącą pracownikiem i współpracownikiem Caalm Clinic Sp. z o.o. , dla której nie istnieją podstawy prawne do nadania jej upoważnienia do przetwarzania danych osobowych

Właściciel zasobów – osoba odpowiedzialna za gromadzenie i przetwarzanie danych osobowych w Klinice,

Klinika – Caalm Clinic Sp. z o.o.

Przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych

Przetwarzanie danych osobowych w systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych

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

Poufność – właściwość zapewniająca, że informacja (np. dane osobowe) jest dostępna jedynie osobom upoważnionym

Rozliczalność – właściwość zapewniająca, że działania Przychodni mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi

Uchybienie - świadome lub nieświadome działania zmierzające do zagrożenia, wskutek których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych

Usuwanie danych - to zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą

Użytkownik - rozumie się przez to osobę, której został przydzielony przez administratora systemu indywidualny identyfikator w systemie informatycznym w powiązaniu z niezbędnymi uprawnieniami dostępowymi w tym systemie, osoba wykorzystująca sprzęt i oprogramowanie do wykonania zadań służbowych

System informatyczny – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych

Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem

Zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie

Zbiór nieinformatyczny – zbiór danych osobowych prowadzony poza systemem informatycznym, w szczególności w postaci papierowej.

Zgoda osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie

§ 3

Deklaracja Administratora

1. Administrator Danych mając świadomość, iż przetwarza dane szczególnych kategorii pacjentów i pracowników deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.

2. Administrator Danych zobowiązuje się do podjęcia odpowiednich kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności aby dane osobowe były:

    a. przetwarzane zgodnie z prawem,

    b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnie z tymi celami,

    c. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

    d. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania

    e. zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność i poufność tych danych.

3. W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator Danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności Polityka Bezpieczeństwa oraz Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych. Dokumenty te są uzupełniane załącznikami do dokumentacji, na które składają się m.in.: wykazy zbiorów, miejsc ich przetwarzania oraz ewidencji osób upoważnionych do przetwarzania danych.

4. Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100% szczelności systemu, konieczne jest, aby każda osoba upoważniona do przetwarzania danych w Klinice, pełna świadomej odpowiedzialności, postępowała zgodnie z przyjętymi zasadami i minimalizowała zagrożenia wynikające z błędów ludzkich.

5. W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

§ 4

Zarządzanie obszarem ochrony danych osobowych

1. Realizację zadań mających na celu zwiększenie skuteczności ochrony danych osobowych powinny zagwarantować następujące założenia:

    - Administrator Danych prowadzi dokumentację opisującą sposób przetwarzania danych zgodnie z obowiązującym prawem
    - do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych
    - Administrator Danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane
    - Administrator Danych lub osoba przez niego upoważniona prowadzi ewidencję osób upoważnionych do ich przetwarzania
    - osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia
    - przeszkolenie wszystkich osób dopuszczonych do przetwarzania danych w zakresie bezpieczeństwa danych osobowych.
    - przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do danych osobowych - stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień.
    - Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. W tym celu prowadzi Rejestr Umów Powierzenia Przetwarzania Danych Osobowych, który stanowi **Załącznik nr 17**

- okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.

- podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych.

- wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania, służących wzmocnieniu bezpieczeństwa przetwarzanych danych osobowych.

2. Ochrona zasobów danych osobowych Kliniki przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników.

3. Na każdym etapie przetwarzania danych osobowych należy brać pod uwagę, w niezbędnym zakresie, integralność, poufność oraz rozliczalność dla przetwarzanych danych osobowych.

4.Inspektor ochrony danych realizując Politykę Bezpieczeństwa ma prawo wydawać zalecenia regulujące kwestie związane z ochroną danych osobowych.

5. W umowach zawieranych przez Klinikę winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych osobowych udostępnionych przez Klinikę.

§ 5

Obowiązki Administratora Danych

1. Administratorem Danych jest Caalm Clinic Sp. z o.o.. reprezentowana przez członków Zarządu dwuosobowo, łącznie czterech członków Zarządu lub członka Zarządu łącznie z Prokurentem, która w rozumieniu przepisów rozporządzenia decyduje o celach i środkach przetwarzania danych osobowych.

2. Administrator Danych jest odpowiedzialny za przetwarzanie danych osobowych w ramach Kliniki oraz obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w

szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. Administrator Danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były: przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem Art. 5 rozporządzenia, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane oraz przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

4. Obowiązkiem spoczywającym na Administratorze oprócz obowiązku dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, jest obowiązek informacyjny (art. 13 i 14 rozporządzenia) oraz obowiązek prawa osoby do kontroli swoich danych i uzyskania informacji o zasadach przetwarzania jej danych osobowych (art. 12 rozporządzenia). Wzór wyrażenia zgody na przetwarzanie danych osobowych stanowi Załącznik nr 14, a obowiązek informacyjny i obowiązek prawa do kontroli przetwarzanych danych osobowych w zbiorach danych stanowi Załącznik nr 15.

5. Do kompetencji Administratora Danych należy w szczególności:

    - określenie celów i procedur ochrony danych osobowych
    - podział zadań i obowiązków związanych z organizacją obszaru ochrony danych osobowych.

6. Do obowiązków Administratora Danych należy:

    - zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych
    - przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych
    - zapewnienie środków finansowych na ochronę pomieszczeń, w których przetwarzane są dane osobowe oraz środków niezbędnych do zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych przetwarzanych w systemach informatycznych i nieinformatycznych.

§ 6

Obowiązki Inspektora Ochrony Danych

1. Inspektor ochrony Danych jest odpowiedzialny za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.

2. Do kompetencji Inspektora Ochrony Danych należy:

    - określenie zasad ochrony danych osobowych.

    - wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.

3. Do obowiązków Inspektora Ochrony Danych należy:

- nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych.

- zapoznawanie pracowników oraz współpracowników z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem.

- prowadzenie rejestru zbiorów danych osobowych zawierającego nazwę zbioru oraz informacje, o których mowa w art. 30 ust. 1 a-c rozporządzenia.

- reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń do Administratora Danych.

- sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.

- aktualizacja posiadanej dokumentacji dot. zasad ochrony danych osobowych tj. Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym, Instrukcji Postępowania w Sytuacji Naruszenia Bezpieczeństwa Danych Osobowych obowiązujących w Klinice.

- prowadzenie dokumentacji związanej z ochroną danych osobowych na podstawie otrzymanych pisemnie informacji od Głównej księgowej , zawierającej:
    - wykaz zbiorów danych osobowych,
    - ewidencje osób upoważnionych do przetwarzania danych osobowych,
    - wykaz obszarów przetwarzania danych osobowych
    - listy przeszkolonych osób,

- sporządzanie raportów wraz z zaleceniami dot. usunięcia nieprawidłowości w systemie bezpieczeństwa ujawnionych podczas prowadzonych przeglądów bezpieczeństwa.

§ 7

Obowiązki Administratora Systemów Informatycznych

Obowiązki Administratora Systemów Informatycznych określone są w umowie zawartej pomiędzy Kliniką a zewnętrzną firmą świadczącą usługi informatyczne.

§ 8

Odpowiedzialność Przedstawiciela Administratora Danych

1. Do kompetencji Przedstawiciela administratora danych należy:

    - określenie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz sposobu ich przetwarzania danych osobowych.

    - określenie sposobu przetwarzania danych osobowych (system informatyczny, system tradycyjny).

2. Do obowiązków Przedstawiciela administratora danych należy:

    - Przekazanie IOD na piśmie informacji dotyczących okresu zatrudnienia lub ustania stosunku pracy pracownika, współpracownika, stażysty, wolontariusza lub innych osób świadczących usługi na rzecz Kliniki.

    - w przypadku utworzenia nowego zbioru danych osobowych ustalenie: kogo dane dotyczą, jaki jest ich zakres (np. imię i nazwisko, adres zamieszkania, NIP, PESEL itp.), cel przetwarzania oraz komu dane osobowe mają być udostępniane. Wszystkie te informacje powinny zostać przekazane IOD przed rozpoczęciem przetwarzania danych.

    - zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia.

    - zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu.

    - realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane.

    - przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku stanowiącym załącznik do zasad udostępnienia dokumentacji medycznej

    - wnioskowanie do Administratora Danych o nadanie lub modyfikację zakresu upoważnień dla pracowników

    - Przedstawiciel administratora danych odpowiada za przygotowanie i nadzór nad umowami powierzenia przetwarzania danych osobowych.

3. Funkcję Właściciela zasobów pełni Andrzej Grabowski

§ 9

Odpowiedzialność pracowników i użytkowników systemu.

1. W celu zapewnienia wysokiego poziomu bezpieczeństwa danych osobowych konieczne jest zaangażowanie każdego pracownika i użytkownika systemu w proces ochrony danych osobowych.

2. Wszyscy pracownicy i użytkownicy powinni być przeszkoleni i poinformowani o spoczywającej na nich odpowiedzialności w zakresie kontroli dostępu oraz zabezpieczenia sprzętu, z którego korzystają.

3. Pracownicy i pozostali użytkownicy odpowiedzialni są za bezpieczeństwo danych, do których mają dostęp zgodnie z przyznanymi upoważnieniami.

Wszyscy pracownicy i użytkownicy systemu zobowiązani są do stosowania:

- **polityki haseł** określonej w § 6 (Metody i środki uwierzytelniania w systemie oraz procedury związane z ich zarządzaniem i użytkowaniem) Instrukcji Zarządzania Systemem Informatycznym.

- **polityki czystego biurka** dla dokumentów papierowych i nośników elektronicznych - w przypadku dłuższej nieobecności przy stanowisku pracy lub po jej zakończeniu pracownik lub użytkownik jest zobowiązany do umieszczenia wszelkich dokumentów i nośników zawierających dane osobowe w bezpiecznym miejscu, np. zamykanej szafce, w celu uniemożliwienia dostępu do nich osobom nieuprawnionym.

- **polityki czystego ekranu** - w przypadku opuszczenia stanowiska pracy pracownik lub użytkownik systemu zobowiązany jest do wylogowania się z aplikacji lub zablokowania dostępu do pulpitu stacji roboczej, w celu uniemożliwienia dostępu do systemu lub aplikacji osoby nieupoważnionej

- **Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie** przeznaczone dla użytkowników systemu określonej w §7 Instrukcji Zarządzania Systemem Informatycznym.

- **procedury korzystania z nośników danych** :

- wyznaczona przez AD osoba prowadzi wykaz wszystkich nośników danych znajdujących się w Klinice - **Załącznik nr 1 do Instrukcji Zarządzania**

Systemem Informatycznym

- nośniki danych przechowuje się w zamkniętych szafkach
- niedozwolone jest podłączanie do komputerów innych nośników danych (pendrive, dyski zewnętrzne, telefony komórkowe), które nie stanowią własności Kliniki. Wyjątek stanowić będą przynoszone przez Pacjentów tylko do odczytu płyty CD/DVD z wynikami ich badań np. opis i zdjęcia RtG, TK
- niedopuszczalne jest kopiowanie danych osobowych w tym danych medycznych na komputery przenośne, telefony komórkowe itd., inne niż zatwierdzone przez Administratora dopuszczone do użytku Kliniki.
- niedopuszczalne jest wyrzucanie nośników danych do kosza. W przypadku zużycia lub uszkodzenia elektronicznego nośnika postępuje się zgodnie z zapisem §8 pkt 5 IZSI
- nośniki, które nie będą już wykorzystywane należy zniszczyć w sposób trwały

6. **Zasady korzystania z urządzeń biurowych**:
    - pracownicy lub użytkownicy systemu korzystający z urządzeń biurowych nie mogą zostawiać żadnych dokumentów zarówno w otoczeniu danego urządzenia jak i wewnątrz urządzeń.
    - urządzenia biurowe powinny znajdować się w miejscu niedostępnym dla osób nieuprawnionych.

7. Do obowiązków pracowników i pozostałych użytkowników należy:
    - informowanie o wszelkich podejrzeniach naruszeniach lub zauważonych naruszeniach Rozporządzenia,
    - znajomość i postępowanie zgodnie z przyjętą Polityką Bezpieczeństwa,
    - znajomość i postępowanie zgodnie z zapisami Instrukcji Zarządzania Systemem Informatycznym,
    - zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
    - ochronę danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,

- ścisłego przestrzegania zakresu nadanego upoważnienia do przetwarzania danych osobowych,

- niezwłoczne informowanie AD o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w Klinice,

- bezwzględnie wykonywanie poleceń AD i ASI w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego,

- utrzymaniu w ścisłej tajemnicy indywidualnych identyfikatorów i haseł dostępu,

- przestrzeganie wszystkich wdrożonych procedur.

8. Pracownicy w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać następujące zasady:

- chronić dane osobowe przed przechwyceniem, kopiowaniem, modyfikacją lub zniszczeniem,

- zachować szczególną ostrożność oraz bezwzględnie nie udostępniać informacji dotyczących danych osobowych w trakcie rozmów telefonicznych,

- nie pozostawiać wiadomości zawierających dane osobowe na automatycznych sekretarkach,

transport danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe, powinien być prowadzony przez osoby upoważnione w sposób ograniczający możliwość ich pozyskania i odczyt przez osoby nieupoważnione.

§ 10

Sankcje prawne za naruszenie zasad ochrony danych osobowych.

1. W przypadku naruszenia przepisów lub zasad postępowania, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej i karnej. Naruszenie zasad ochrony danych osobowych a także sposobu ich zabezpieczania, może skutkować postawieniem takiej osobie zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Rozporządzenia lub przestępstwa określonego w art. 266 Kodeksu Karnego.

§ 11

Wykaz miejsc przetwarzania

Wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych. Wyznaczają go pomieszczenia zlokalizowane w Klinice. Szczegółowy wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe opisany został w **Załączniku nr 1.**

§ 12

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Wykaz zbiorów osobowych wraz ze wskazaniem programów komputerowych służących do ich przetwarzania przedstawiony został zgodnie z **Załącznikiem nr 2** do niniejszej dokumentacji. Z uwagi na połączenie komputerów z siecią Internet, dla zbiorów przetwarzanych elektronicznie stosuje się, środki bezpieczeństwa na poziomie **WYSOKIM**.

§ 13

Środki organizacyjne i techniczne ochrony danych osobowych

1. Administrator Danych zobowiązany jest zapewnić zastosowanie środków technicznych oraz organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych. Środki ochrony opisane są w **Załączniku nr 3**.

§ 14

Zasady ochrony zbiorów nieinformatycznych.

1. Zbiory nieinformatyczne winny być odpowiednio zabezpieczone przed utratą, kradzieżą, zniszczeniem lub nieuprawnionym dostępem.

2. Dokumenty i wydruki zawierające dane osobowe należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.

3. Na czas nieużytkowania dokumenty i wydruki zawierające dane osobowe winny być zamykane w szafkach biurowych lub szufladach.

4. Wydruki robocze, błędne lub zdezaktualizowane winny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

§ 15

Dopuszczenie do przetwarzania danych osobowych / ewidencja osób upoważnionych.

1. Pracownicy i współpracownicy mają prawo do przetwarzania danych osobowych wyłącznie po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych, wystawionego przez Administratora Danych.

2. W tym celu Administrator Danych przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:

    - zapoznaje pracownika z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w Klinice

    - wystawia pracownikowi formalne upoważnienie do przetwarzania danych osobowych, zgodnie ze wzorem upoważnienia stanowiącym **Załącznik nr 4** do niniejszej Polityki

    - upoważnienie do przetwarzania danych w systemie informatycznym nadawane jest na podstawie uprawnień użytkownika. Szczegółowa procedura znajduję się w § 5 IZSI

    - przyjmuje od pracownika podpisane oświadczenie o zachowaniu w poufności danych osobowych i sposobów ich zabezpieczenia, zgodnie ze wzorem oświadczenia stanowiącym **Załącznik nr 5** do niniejszej Polityki

    - Oryginały upoważnień do przetwarzania danych osobowych i oświadczeń o zachowaniu poufności i przestrzeganiu zatwierdzonych procedur bezpieczeństwa będą przechowywane w prowadzonej dokumentacji ochrony danych osobowych.

3. Osoby upoważnione do przetwarzania danych osobowych wpisywane są do ewidencji na podstawie nadawanych **uprawnień użytkownika w systemie informatycznym**, który stanowi załącznik nr 2 do IZSI.

4. Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest przez Inspektora Ochrony Danych i na podstawie pisemnie przekazanych informacji przez AD lub Właściciela zasobów i zawiera:

    - imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych.

    - zakres upoważnienia do przetwarzania danych osobowych.

    - identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych.

    - datę nadania i odebrania uprawnień.

5. Ewidencja osób upoważnionych do przetwarzania danych osobowych przechowywana jest na terenie Kliniki, do której dostęp ma Administrator Danych, Właściciel Zasobów i Inspektor Ochrony Danych

Wzór karty z ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi **Załącznik nr 6** do niniejszej Polityki.

§ 16

Wykaz zbiorów danych osobowych.

1. Właściciel zasobów jest zobowiązany zgłosić Inspektorowi Ochrony Danych zamiar utworzenia nowego zbioru danych osobowych wraz z wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych.

2. Inspektor Ochrony Danych weryfikuje utworzenie nowego zbioru danych osobowych, analizuje nowy zbiór danych oraz prowadzi rejestr zbiorów danych przetwarzanych przez Administratora Danych, brak obowiązku rejestracji zbioru danych w PUODO.

3. Inspektor Ochrony Danych uzupełnia Politykę, dokumenty z nią powiązane oraz pozostałe dokumenty obowiązujące w przedsiębiorstwie w zakresie ochrony danych osobowych o informacje na temat nowego zbioru.

§ 17

Opis struktury zbiorów danych osobowych i sposób przepływu danych pomiędzy poszczególnymi systemami

1. Dane osobowe mogą być przetwarzane w zbiorach danych, przy zastosowaniu systemów informatycznych oraz zbiorów ewidencyjnych w postaci kartotek, skorowidzów, wydruków, ksiąg i wykazów.

2. Zawartość pól informacyjnych występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa.

3. Administrator Danych prowadzi ewidencję stosowanych systemów i programów, zastosowanych do przetwarzania danych osobowych – **Załącznik nr 7**

4. Dla każdego zidentyfikowanego zbioru danych zostaje wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze. Opis poszczególnych pól informacyjnych w strukturze zbioru danych przedstawia **Załącznik nr 8.**

5. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych opisuje **Załącznik nr 9.**

§ 18

Udostępnienie danych osobowych

1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

2. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

3. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie wniosku określonym w "Procedurze udostępniania dokumentacji medycznej", a jeśli wniosek nie dotyczy informacji objętych dokumentacją medyczną - w terminie 30 dni od daty złożenia wniosku. Wniosek o udostępnienie dokumentacji medycznej stanowi załącznik do „Procedury udostępniania dokumentacji medycznej”.

4. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku odpowiedzialne są osoby wskazane w wykazie stanowiącym **Załącznik nr 16 Polityki Bezpieczeństwa.**

§ 19

Powierzanie danych osobowych

1. Administrator Danych powierza dane osobowe do przetwarzania w formie usługi zewnętrznej podmiotom zewnętrznym w oparciu o umowę powierzenia przetwarzania danych. Podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie powierzenia przetwarzania danych osobowych.

1. Powierzenie może mieć miejsce wyłącznie w trybie przewidzianym zapisami art. 28 Rozporządzenia RODO poprzez podpisanie stosownej pisemnej umowy powierzenia pomiędzy Administratorem Danych a podmiotem, któremu powierzono przetwarzanie danych osobowych.

2. Podmiot któremu powierzono przetwarzanie danych osobowych może przetwarzać te dane wyłącznie w zakresie i celu przewidzianym w umowie o której mowa w ust. 1§2 .

3. W celu uporządkowania i bieżącego monitorowania Administrator Danych lub wyznaczona przez niego osoba prowadzi rejestr Umów Powierzenia Przetwarzania Danych Osobowych, który stanowi **Załącznik nr 17**

4. Za przygotowanie i nadzór nad umowami powierzenia odpowiada Andrzej Grabowski

§ 20

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik i inny użytkownik danych osobowych, który stwierdzi zagrożenie ochrony danych osobowych lub naruszenie ich bezpieczeństwa zobowiązany jest do natychmiastowego poinformowania o tym Inspektora ochrony

Danych oraz Administratora Danych oraz zastosować się do Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w systemie informatycznym opisanych w **Załączniku nr 12.**

2. W przypadku stwierdzenia uchybienia/naruszenia dotyczącego ochrony danych osobowych AD prowadzi postępowanie wyjaśniające, w toku którego ustala zakres i przyczyny oraz jego ewentualne skutki, a także wskazuje jakie działania naprawcze i zapobiegawcze powinny zostać podjęte w celu wyeliminowania podobnych uchybień w przyszłości. Wszystkie stwierdzenia uchybień/naruszeń AD opisuje w raporcie, który stanowi **Załącznik nr 11**

3. W przypadku stwierdzenia zagrożenia ochrony danych osobowych AD prowadzi postępowanie wyjaśniające, w toku którego ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki, a także wskazuje jakie działania naprawcze i zapobiegawcze powinny zostać podjęte w celu wyeliminowania podobnych zagrożeń w przyszłości.

4. W przypadku naruszenia bezpieczeństwa danych osobowych AD prowadzi postępowanie wyjaśniające, w toku którego ustala czas i miejsce naruszenia, jego zakres, przyczyny, skutki, w tym wielkość szkód które naruszenie spowodowało, zabezpiecza dowody, podejmuje działania w celu ustalenia sprawcy naruszenia oraz powiadamia Administratora Danych o wynikach postępowania i wskazuje mu jakie działania naprawcze i zapobiegawcze powinny zostać podjęte w celu wyeliminowania podobnych zagrożeń w przyszłości;

§ 21

Postanowienia końcowe

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą która dopuściła się naruszenia.

2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy Rozporządzenia oraz przepisy wykonawcze do tego Rozporządzenia.

Integralną część Polityki stanowią załączniki:

- **Załącznik nr 1** - Szczegółowy wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe
- **Załącznik nr 2** - Wykaz zbiorów danych osobowych
- **Załącznik nr 3 -** Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych
- **Załącznik nr 4** - Upoważnienie do przetwarzania danych osobowych
- **Załącznik nr 5** - Oświadczenie
- **Załącznik nr 6** - Karty z ewidencji osób upoważnionych do przetwarzania danych osobowych
- **Załącznik nr 7** – Ewidencja stosowanych systemów i programów
- **Załącznik nr 8** – Opis struktury zbioru i zakres informacji poszczególnych w zbiorze
- **Załącznik nr 9** - Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych
- **Załącznik nr 10 –** Wzór zgody na przebywanie w pomieszczeniach dla osób nie posiadających upoważnienia
- **Załącznik nr 11 –** Wzór raportu z uchybienia/naruszenia bezpieczeństwa zasad ochrony danych osobowych
- **Załącznik nr 12-** Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w systemie informatycznym
- **Załącznik nr 13 -** Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń
- **Załącznik nr 14** – Wzór wyrażenia zgody na przetwarzanie danych osobowych
- **Załącznik nr 15** – Obowiązek informacyjny i obowiązek prawa do kontroli przetwarzanych danych osobowych w zbiorach danych
- **Załącznik nr 16 –** Wykaz osób odpowiedzialnych za przygotowanie danych osobowych do udostępnienia
- **Załącznik nr 17** – Rejestr Umów Powierzenia Danych Osobowych
- **Załącznik nr 19 –** Dziennik wejść/wyjść z Archiwum