POLITYKA OCHRONY DANYCH

Hemoklinika Sp. z o.o.
ul. Stanisławy Leszczyńskiej 18 lok. 2
93-347 Łódź

Wydanie 1 z dnia 18.05.2022

Zatwierdzona przez …….
(podpis zgodnie z zasadami reprezentacji)

SPIS TREŚCI

PODSTAWOWE POJĘCIA I SKRÓTY

1. Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z Ustawa o ochronie danych osobowych (zwana dalej UODO)– Ustawa z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000.)
2. Rozporządzenie RODO (zwane dalej RODO)- Rozporządzenie przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, s. 1)

3. Przepisy o ochronie danych osobowych- przepisy ustawy o ochronie danych osobowych oraz wszelkie właściwe powiązane lub pochodne regulacje i wytyczne dotyczące przetwarzania i ochrony danych osobowych
4. UODO- Urząd Ochrony Danych Osobowych
5. Administrator- osoba fizyczną lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art.4 pkt.7 RODO).
6. Inspektor Ochrony Danych (IOD) osoba powołana na podstawie art. 37 ust. 1 RODO wykonująca swoje zadania zgodnie z art. 39 RODO
7. Administrator Systemu Informatycznego (ASI) - podmiot, osoba odpowiedzialna za techniczno-organizacyjną obsługę systemu teleinformatycznego
8. Dane osobowe- 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
9. Przetwarzanie danych– operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
10. Zbiór danych osobowych– (art. 4 pkt. 6 RODO) oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
11. Dokument elektroniczny- zbiór danych, stanowiący odrębną całość znaczeniową, uporządkowany w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych.
12. System teleinformatyczny– zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z 16 lipca 2004 r.– Prawo telekomunikacyjne (Dz.U. 2004 nr 171 poz. 1800).
13. Środki komunikacji elektronicznej rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi (w szczególności poczta elektroniczna)
14. System tradycyjny– zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych w formie papierowej.
15. Zabezpieczenie danych w systemie teleinformatycznym wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mające na celu w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą uszkodzeniem lub zniszczeniem.
16. Osoba uprawniona do przetwarzania danych osobowych – osoba, która została upoważniona przez Administratora do przetwarzania danych osobowych; dotyczy to osób zatrudnionych, świadczących usługi na podstawie umów cywilno-prawnych jak i innych, np. stażystów, wolontariuszy, praktykantów, itp.
17. Użytkownik systemu teleinformatycznego – osoba, upoważniona przez Administratora, do przetwarzania danych osobowych w systemie informatycznym, która odbyła stosowne szkolenie z zakresu ochrony tych danych.
18. Identyfikator użytkownika (login)– ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
19. Hasło– ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
20. Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

21. Usunięcie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
22. Integralność danych– funkcjonalność zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
23. Integralność systemu – nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.
24. Poufność danych– funkcjonalność zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
25. Rozliczalność- funkcjonalność zapewniająca, że określone działanie dowolnego podmiotu jest jednoznacznie przypisane temu podmiotowi oraz zgodność z regulacją RODO
26. Dostępność informacji - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, kiedy jest to potrzebne.
27. Zarządzanie ryzykiem- proces identyfikowania, kontrolowania, minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa aktywów służących do przetwarzania i ochrony danych osobowych, w szczególności systemów teleinformatycznych służących do przetwarzania danych osobowych.
28. Podmiot przetwarzający/Procesor- osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art.4 pkt.8 RODO).
29. Naruszenie ochrony danych osobowych (incydent bezpieczeństwa)- 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 (art.4 pkt.12 RODO).
30. Zgoda osoby, której dane dotyczą- dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, przyzwala, w formie oświadczenia lub wyraźnego działania potwierdzającego, na przetwarzanie dotyczących jej danych osobowych (art.4 pkt.11 RODO).
31. Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych

WPROWADZENIE

§1.

1. Niniejsze wydanie Polityki Ochrony Danych jest efektem wdrożenia zasad 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) (Dz. Urz. UE L 119 z 04.05.2016, s. 1)
2. Celem Polityki Ochrony Danych jest zapewnienie ochrony danych osobowych przetwarzanych przez Hemoklinika Spółka z ograniczoną odpowiedzialnością z siedzibą w Łodzi (93-347) przy ul. Stanisławy Leszczyńskiej 18 lok. 2 wpisanej do Krajowego Rejestru Sądowego – Rejestru Przedsiębiorców pod numerem KRS 0000810211, posiadającą NIP: 7292732327, nr REGON: 384710876 (zwaną dalej **Hemoklinika** lub zamiennie **Administrator**) przed zagrożeniami wewnętrznymi i zewnętrznymi poprzez optymalny i zgodny z wymogami obowiązujących aktów prawnych, sposób przetwarzania informacji zawierających dane osobowe.
3. Polityka Ochrony Danych ma zastosowanie do przetwarzania danych osobowych w szczególności w związku z realizacją:
   1) zadań wynikających z przepisów prawa krajowego oraz Unii Europejskiej i określonych szczegółowo w Regulaminie Organizacyjnym;
   2) obowiązków pracodawcy w rozumieniu Kodeksu pracy;
   3) obowiązków wynikających z umów kontraktowych
   4) umów o organizację staży, praktyk, wolontariatu;
   5) udzielania świadczeń zdrowotnych
4. Zapewnienie ochrony danych osobowych w **Hemoklinika** jest rozumiane jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie.
5. Dokument Polityka Ochrony Danych opisuje procedury zapewnienia bezpieczeństwa przetwarzanych danych osobowych, oraz postępowanie dla zapobiegania skutkom zagrożeń.
6. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych, a zarządzanie ryzykiem rozumiane jest jako proces identyfikowania, oceny, kontrolowania i postępowania z ryzykiem

dotyczącym bezpieczeństwa przetwarzanych danych osobowych.

§2.

Politykę Ochrony Danych stosuje się w szczególności do:

1. Danych osobowych przetwarzanych w systemach informatycznych;
2. Wszystkich informacji dotyczących danych osobowych zawartych w przetwarzanych zbiorach;
3. Wszystkich lokalizacji - budynków i pomieszczeń, w których są przetwarzane dane osobowe;
4. Wszystkich informacji danych zawartych w opisie struktury zbiorów;
5. Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;
6. Rejestru osób uprawnionych do przetwarzania danych osobowych;
7. Innych dokumentów zawierających dane osobowe.

§3.

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki Ochrony Danych mają zastosowanie do wszystkich systemów, 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 - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
   3) wszystkich pracowników, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki Ochrony Danych zobowiązani są wszyscy pracownicy, w tym inne osoby mające dostęp do informacji podlegających ochronie.

§4.

Opracowanie Polityki Ochrony Danych wynika w szczególności z przepisów:

1. 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) (Dz. Urz. UE L 119 z 04.05.2016, s. 1);
2. Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000.);
3. Ustawy o systemie informacji w ochronie zdrowia z dnia 28 kwietnia 2011 (Dz.U. z 2011r., poz. 657 z późn. zm.)
4. Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta- z dnia 4 maja 2020 (Dz.U. 2020 poz. 849).

§5.

1. **Hemoklinika** ma świadomość znaczenia przetwarzanych danych osobowych, przykłada najwyższą wagę do zapewnienia im odpowiedniego poziomu bezpieczeństwa, ponieważ mają one fundamentalne znaczenia dla

realizacji misji i celów statutowych, a ich zgodne z prawem wykorzystanie pozwala na wzmocnienie reputacji.
2. Dane osobowe stanowią kluczowe zasoby informacyjne **Hemoklinika** i zapewnia się im odpowiednią ochronę.
3. Polityka Ochrony Danych dotyczy wszystkich danych osobowych przetwarzanych w **Hemoklinika**, niezależnie od formy ich przetwarzania (system tradycyjny, systemy teleinformatyczne).
4. Opisane reguły obowiązują wszystkie osoby uprawnione do przetwarzania danych osobowych oraz podmioty współpracujące na podstawie umowy cywilnoprawnej, które mają jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

OBOWIĄZEK INFORMACYJNY

Zgodnie z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych informujemy że:

1. Administratorem Państwa danych osobowych jest Hemoklinika Spółka z o. o. z siedzibą w Łodzi (93-347) przy ul. Stanisławy Leszczyńskiej 18 lok. 2, którą reprezentuje Zarząd Spółki.
2. We wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych można się kontaktować z Administratorem lub wyznaczonym Inspektorem Ochrony Danych pod adresem poczty elektronicznej biuro@hemoklinika.pl lub pisemnie na adres siedziby Administratora.
3. Państwa dane osobowe przetwarzane są w celach:
   1) udzielania świadczeń zdrowotnych służących ochronie zdrowia i życia oraz udostępniane w tym celu innym podmiotom na podstawie obowiązujących szczególnych przepisów prawa:
   2) realizacji umów i działań podjętych na Państwa życzenie, lub których jesteście Państwo stroną (art. 6 ust. 1 lit. b RODO);
   3) zapewnienie bezpieczeństwa i porządku oraz ochrony osób i mienia
   4) archiwalnych, naukowych lub statystycznych
   5) związanych z prowadzeniem ksiąg rachunkowych i dokumentacji podatkowej
4. Odbiorcami Państwa danych osobowych mogą być:
   1) organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa;
   2) inne podmioty, które na podstawie stosownych umów/porozumień zawartych z **Hemokliniką** przetwarzają dane osobowe dla których Administratorem jest **Hemoklinika.**
5. Państwa dane osobowe będą przechowywane jedynie w okresie niezbędnym do spełnienia celu, dla którego zostały zebrane, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa.
6. W związku z przetwarzaniem Państwa danych osobowych przysługują Państwu następujące prawa:
   1) dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
   2) żądania sprostowania (poprawiania) danych osobowych w przypadku, gdy dane są nieprawidłowe lub niekompletne;
   3) żądania usunięcia danych osobowych (prawo do bycia zapomnianym), w przypadku gdy dane przetwarzane są na podstawie zgody i mogą być usunięte po zakończeniu okresu archiwizacji.
   4) żądania ograniczenia przetwarzania danych osobowych pod warunkiem, że osoba, której dane dotyczą wykaże jedną z podstaw prawnych w art.18 ust.1 a-d RODO.
   5) prawo sprzeciwu wobec przetwarzania danych z wyłączeniem w przypadków, gdy **Hemoklinika** posiada uprawnienie do przetwarzania danych na podstawie przepisów prawa.
   6) prawo do przenoszenia danych w przypadku, gdy łącznie spełnione są następujące przesłanki:
      a) przetwarzanie danych odbywa się na podstawie umowy zawartej z osobą, której dane dotyczą lub na podstawie zgody wyrażonej przez tę osobę,
      b) przetwarzanie odbywa się w sposób zautomatyzowany i Administrator posiada odpowiednie możliwości techniczne i organizacyjne do dokonania przeniesienia danych

7. W przypadku gdy przetwarzanie danych osobowych odbywa się na podstawie zgody osoby, której te dane dotyczą (art. 6 ust. 1 lit a RODO), przysługuje Państwu prawo do cofnięcia tej zgody w dowolnym momencie. Cofnięcie to nie ma wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
8. W przypadku uznania, że przetwarzanie Państwa danych osobowych narusza przepisy o ochronie danych osobowych, przysługuje Państwu prawo do wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.
9. Podanie przez Państwa danych osobowych jest obowiązkowe, w sytuacji gdy przesłankę przetwarzania danych osobowych stanowi przepis prawa lub zawarta między stronami umowa.
10. Państwa dane osobowe nie będą przetwarzane w sposób zautomatyzowany i nie będą profilowane.

ZADANIA ADMINISTRATORA

1. Administrator stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do **zagrożeń** oraz **kategorii danych** objętych ochroną. Administrator zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem
2. 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 rozporządzeniem RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
3. Administrator dokłada wszelkich starań, aby przetwarzane dane osobowe były bezpieczne. W tym celu stosowane są rozwiązania techniczne i organizacyjne, które mają za zadanie zabezpieczenie danych osobowych. Tymi środkami są w szczególności: regularne testowanie infrastruktury teleinformatycznej pod kątem bezpieczeństwa, kontrolowanie dostępu do danych, metody kryptograficzne.
4. W zakresie zadań realizowanych w pkt 1 Administrator w szczególności:
   1) prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki organizacyjne i techniczne zabezpieczające dane osobowe;
   2) nadaje upoważnienia do przetwarzania danych i dopuszcza do pracy wyłącznie osoby posiadające takie upoważnienie;
   3) **zapewnia kontrolę** nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane;
   4) prowadzi ewidencję osób upoważnionych do ich przetwarzania**,** która zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a także identyfikator, jeżeli dane są przetwarzane w systemie teleinformatycznym;
   5) nadaje i odwołuje upoważnienia do przetwarzania danych osobowych
   6) czuwa nad stosowaniem i przestrzeganiem przepisów obowiązujących aktów prawnych oraz nadzoruje pracę dodatkowych osób odpowiedzialnych za bezpieczeństwo przetwarzanych danych osobowych;
   7) dokonuje, przed rozpoczęciem przetwarzania, oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych DPIA (*data protection impact assessment)* w sytuacji kiedy dany rodzaj przetwarzania– w szczególności z użyciem nowych technologii– ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw wolności osób fizycznych,
   8) zgłasza naruszenia ochrony danych osobowych organowi nadzorczemu oraz informuje o tym osobę, której to naruszenie dotyczy, w formie i trybie zgodnym z art. 33 RODO;
   9) zarządza ryzykiem ochrony danych osobowych, zgodnie z podejściem *risk based approach* i dokumentuje proces;
   10) prowadzi rejestr czynności przetwarzania.

ZADANIA INSPEKTORA OCHRONY DANYCH (ART. 39 RODO)

1. Inspektor ochrony danych ma następujące zadania

1) informowanie Administratora, podmiotu przetwarzającego oraz osób, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia osób uczestniczących w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania danych, mając na uwadze charakter, zakres, kontekst i cele przetwarzania danych.

REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada.
2. Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora.
3. Zakres informacji zawartych w powyższych rejestrach określony jest w art. 30 rozporządzenia RODO.
4. Rejestr czynności przetwarzania zawarty jest w załączniku do Polityki Ochrony Danych.

ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARANYCH DANYCH

§1.

1. **Hemoklinika** stosuje odpowiednie środki informatyczne, techniczne, organizacyjne zapewniające ochronę przetwarzanych danych osobowych, które są odpowiednie do stopnia zagrożeń oraz kategorii danych objętych ochroną. **Hemoklinika** zabezpiecza dane osobowe przed:
   1) udostępnieniem ich osobom nieupoważnionym,
   2) zabraniem przez osobę nieuprawnioną,
   3) utratą dostępu do danych,
   4) przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem.

§2.

Zabezpieczenia organizacyjne:

1. Sporządzenie i wdrożenie Polityki Ochrony Danych.
2. Sporządzenie i wdrożenie Instrukcji Zarządzania Systemem Informatycznym.
3. Dopuszczenie do przetwarzania danych wyłącznie osób posiadających upoważnienia nadane przez Administratora.
4. Stworzenie instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych.
5. Zaznajomienie osób zatrudnionych przy przetwarzaniu danych z przepisami dotyczącymi ochrony danych osobowych oraz zabezpieczeniami systemu teleinformatycznego.
6. Zobowiązanie osób zatrudnionych przy przetwarzaniu danych osobowych do zachowania w tajemnicy informacji o przetwarzanych danych.
7. Przetwarzanie danych osobowych w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
8. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających

bezpieczeństwo tych danych.
9. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
10. Wprowadzenie zasady „czystego biurka" i „białej kartki".
11. Neutralizacja dokumentów i nośników informacji zawierających dane osobowe, które podlegają zniszczeniu, za pomocą urządzeń do tego przeznaczonych lub modyfikacja która nie pozwala na odtworzenie ich treści.
12. Udzielanie informacji telefonicznych po uprzednim zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych.

§3.

Zabezpieczenia techniczne:

1. Wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą zapory sieciowej Firewall.
2. Stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową; w efekcie zapewnione jest zabezpieczenie sieci przed atakiem z zewnątrz.
3. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem używanych aplikacji.
4. Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika.
5. Komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła.
6. W systemie informatycznym zastosowano autoryzację użytkownika. Autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym zalogowaniu się do systemu informatycznego.

§4.

Środki ochrony fizycznej:

1. Przetwarzanie danych osobowych dokonywane jest w wydzielonych, odpowiednio zabezpieczonych i przystosowanych do tego pomieszczeniach lub częściach pomieszczeń.
2. Pomieszczenia wyposażono w szafki, zamykane na klucz, dające gwarancję bezpieczeństwa dokumentacji i nośników danych.
3. Urządzenia służące do przetwarzania danych osobowych i dokumentację zawierającą dane osobowe umieszcza się w zamykanych pomieszczeniach;
4. Obszar, w którym przetwarzane są dane osobowe, chroniony jest poprzez zastosowanie drzwi zamykanych na klucz, alarm antywłamaniowy.
5. Obszary przetwarzania danych osobowych zabezpieczone są przed pożarem, zalaniem zgodnie z oddzielną procedurą.

§5.

Wynoszenie akt i dokumentacji:

1. Poza miejscami przetwarzania danych nie wolno wynosić żadnej dokumentacji ani akt związanych z wykonywaniem czynności służbowych, a zwłaszcza dokumentów zawierających dane osobowe.
2. Przepis powyższy nie dotyczy tych osób, których zakres obowiązków wymaga dokonywania czynności służbowych z dokumentacją zawierającą dane osobowe poza obszarem przetwarzania danych, a także czynności związanych z przesyłaniem i transportem korespondencji.
3. Osoby, o których mowa w pkt. 2 są zobowiązane stosować środki zapewniające ochronę powierzonych danych osobowych podczas ich transportu, przechowywania i użytkowania poza obszarem siedziby Administratora, a w szczególności zabezpieczyć te dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Osoby, o których mowa w pkt. 2 ponoszą pełną odpowiedzialność za powierzony im sprzęt oraz dokumentację znajdującą się poza siedzibą Administratora.
5. Każda osoba, który podejrzewa, że mogło nastąpić naruszenie bezpieczeństwa ochrony danych osobowych lub próba dokonania takiego naruszenia przez osoby nieupoważnione, jest zobowiązana do niezwłocznego

poinformowania o powyższym Administratora, który prowadzi postępowanie kontrolne, pod kątem wyjaśnienia okoliczności ewentualnego naruszenia bezpieczeństwa danych osobowych.

6. Odpowiedzialność za bezpieczeństwo dokumentacji lub akt wynoszonych poza obszar przetwarzania danych ponosi osoba, która te akta wynosi, z chwilą ich pobrania. Odpowiedzialność ta dotyczy również danych znajdujących się na nośnikach cyfrowych.
7. Po zwrocie akt i dokumentacji (lub przenośnych urządzeń) przez osobę, przełożony tej osoby jest zobowiązany jest do sprawdzenia akt i dokumentacji pod kątem zgodności ze stanem przed wypożyczeniem.
8. Pozostawanie w pracy po godzinach pracy może mieć miejsce tylko w związku z pełnionymi obowiązkami i za zgodą Administratora lub osoby przez niego upoważnionej.
9. Każda osoba po zakończeniu pracy zobowiązana jest zamknąć w szafach wszelką dokumentację oraz urządzenia przenośne (w przypadku ich używania), a następnie osobiście zabezpieczyć klucze z zachowaniem wszelkich zasad bezpieczeństwa.

§5.

Pozostałe zabezpieczenia:

1 Zapoznanie każdej osoby, przed jej przystąpieniem do pracy przy przetwarzaniu danych osobowych, z przepisami dotyczącymi ochrony danych osobowych.
2 Prowadzenie rejestru czynności przetwarzania danych osobowych.
3 Prowadzenie dokumentacji zarządzania ryzykiem (szacowanie, postępowanie i monitorowanie ryzyka).
4 Prowadzenie rejestru incydentów oraz zgłoszeń incydentów bezpieczeństwa.
5 Organizowanie regularnych szkoleń dla osób przetwarzających dane osobowe w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych, obowiązujących standardów ochrony danych osobowych i aktualnych przepisów wykonawczych. Administrator prowadzi w tym celu rejestr zawarty w załączniku do Polityki Ochrony Danych.
6 Podpisanie przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i zrozumieniu treści szkolenia oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
7 Okresowe sprawdzanie, zgodnie z podejściem opartym na analizie ryzyka, w razie konieczności, lecz nie rzadziej niż raz w roku i przynajmniej raz na 5 lat wszystkich zabezpieczeń zbiorów danych w tym systemów informatycznych służących do ich przetwarzania.
8 Kontrolowanie otwierania i zamykania pomieszczeń, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę i niepozostawianiu pomieszczenia w czasie pracy bez nadzoru. Osobami upoważnionymi do przetwarzania danych osobowych są osoby wyszczególnione w załączniku stanowiącym integralną część Polityki Ochrony Danych.
9 Odbieranie pisemnego oświadczenia każdej osoby upoważnionej do przetwarzania danych osobowych, przed przystąpieniem do pracy, że została zaznajomiona z przepisami ustawy UODO i regulacją RODO, aktami wykonawczymi oraz, że rozumie zasady dotyczące ochrony danych osobowych opisane w Polityce Ochrony Danych, Instrukcji Zarządzania Systemem Informatycznym i zobowiązuje się do ich przestrzegania.
10 Zapewnienie przestrzegania wszelkich wewnętrznych regulaminów i instrukcji dotyczących bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualnych zakresów zadań osób zatrudnionych przy przetwarzaniu danych osobowych, w tym zawartych w niniejszej Polityce Ochrony Danych.

POWIERZENIE I UDOSTĘPNIENIE DANYCH OSOBOWYCH

1 **Hemoklinika** na podstawie umów zawartych w formie pisemnej, powierza podmiotom zewnętrznym przetwarzanie danych osobowych w zakresie objętym tymi umowami.
2 Podmioty zewnętrzne zobowiązują się przetwarzać powierzone im dane osobowe zgodnie z rozporządzeniem RODO, rozporządzeniami wykonawczymi oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3 Z uwagi na zawarte umowy z podmiotami zewnętrznymi, w szczególności dotyczące utrzymania infrastruktury informatycznej, Administrator może przekazywać dane osobowe poza Europejski Obszar Gospodarczy. Przekazywanie danych osobowych odbywa się, w takim przypadku, na podstawie odpowiednich mechanizmów prawnych takich jak standardowe klauzule umowne, reżim Privacy Shield lub inne podobne instrumenty prawne przewidziane w RODO.
4 **Hemoklinika** może udostępnić dane osobie wnioskującej z zachowaniem zasady, że udostępnienie danych

osobowych nie może naruszać praw i wolności osoby, których dane dotyczą.

5 Dane osobowe przetwarzane zgodnie z regulacją RODO, mogą być udostępnione jedynie w formie udokumentowanego wniosku osoby, której dane dotyczą lub wniosku osoby upoważnionej przez zainteresowanego.
6 Każdorazowe udostępnienie danych powinno być odnotowane w rejestrze udostępnień, który stanowi załącznik do Polityki Ochrony Danych.
7 Powierzenie przetwarzania danych uregulowane w Polityce Ochrony Danych nie ma zastosowania do udostępniania danych podmiotom upoważnionym do ich przetwarzania w zakresie uregulowanym szczegółowymi przepisami prawa, w tym w szczególności ZUS, Prokuraturze, Policji, Sądom.
8 Wykaz podmiotów, którym powierzono przetwarzanie danych stanowi załącznik do Polityki Ochrony Danych.
9 Ewidencja udostępnionych danych zawarta jest w załączniku do Polityki Ochrony Danych.

OPIS ZDARZEŃ NARUSZAJĄYCH OCHRONĘ DANYCH OSOBOWYCH

Podział zagrożeń:

1 Zagrożenia losowe zewnętrzne (itp. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona, lecz nie dochodzi do naruszenia poufności danych;
2 Zagrożenia losowe wewnętrzne (itp. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych oraz okresowy lub stały brak dostępu do danych;
3 Zagrożenia zamierzone, świadome i celowe- najpoważniejsze zagrożenia, gdzie występują naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

Naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to w szczególności:

1 Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, takie jak wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
2 Niewłaściwe parametry środowiska, takie jak nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
3 Awaria sprzętu lub oprogramowania, w wyniku umyślnego działania;
4 Pojawienie się komunikatu alarmowego z tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
5 Pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
6 Naruszenie lub próba naruszenia integralności systemu lub bazy danych w systemie;
7 Próba modyfikacji lub modyfikacja danych bez odpowiedniego upoważnienia (autoryzacji);
8 Ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
9 Nieautoryzowane konta dostępu do danych;
10 Podmiana, niszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia;
11 Kasowanie lub kopiowanie w sposób niedozwolony danych osobowych;
12 Nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych;
13 Kradzież nośników, na których zapisane są dane osobowe;
14 Rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, kopiarce, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp.);
15 Nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy,

folii, zdjęciach, dyskietkach w formie niezabezpieczonej.

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Każda osoba uprawniona do przetwarzania danych osobowych, w przypadku podejrzenia naruszenia lub faktu naruszenia zasad ochrony danych osobowych, ma obowiązek do natychmiastowego powiadomienia bezpośredniego przełożonego o zaistniałej sytuacji.
2. Zgłoszenie jest przekazywane bezpośrednio przez osobę uprawnioną, która stwierdziła podatność na zagrożenie lub powstały incydent.
3. Informacja jest przekazywana przez osobę upoważnioną w zależności od pory i sytuacji zgodnie ze szczegółową wewnętrzną procedurą. Droga przekazania informacji zależy przede wszystkim od subiektywnej oceny wagi sytuacji dokonanej przez osobę uprawnioną i decyzji jaką podejmie.
4. Po otrzymaniu powiadomienia należy niezwłocznie:
    1) sprawdzić stan urządzeń wykorzystywanych do przetwarzania danych osobowych;
    2) sprawdzić sposób działania programów (w tym obecność wirusów komputerowych);
    3) sprawdzić jakość komunikacji w sieci telekomunikacyjnej;
    4) sprawdzić zawartość zbioru danych osobowych;
    5) przeanalizować metody pracy osób uprawnionych do przetwarzania danych osobowych.
5. W przypadku zaistnienia incydentu Administrator wdraża postępowanie zgodnie z procedurą oceny skutków ochrony danych DPIA *Data Protection Impact Assesment*
6. Działania, w przypadku stwierdzenia incydentu, polegają w szczególności na:

    1) uniemożliwieniu dalszego naruszenia bezpieczeństwa przetwarzanych danych osobowych (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.);
    2) powstrzymaniu lub ograniczeniu dostępu do danych osoby niepowołanej poprzez: fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej, wylogowanie użytkownika podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania;
    3) zabezpieczeniu i utrwaleniu wszelkich informacji i dokumentów mogących stanowić pomoc przy ustaleniu przyczyn naruszenia;
    4) niezwłocznym przywróceniu prawidłowego stanu działania systemu;
    5) dokonaniu analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia;
    6) wydrukowaniu na bieżąco wszystkich możliwych dokumentów i raportów, które mogą pomóc w ustaleniu okoliczności zdarzenia;
    7) sporządzenia szczegółowego raportu zawierającego w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzeń (w załączniku do Polityki Ochrony Danych).
7. Dalsze postępowanie w przypadku zaistnienia incydentu obejmuje następujące działania:
    1) działanie korekcyjne– działanie w celu wyeliminowania skutków powstałego incydentu/ zdarzenia;
    2) działanie korygujące– działanie w celu wyeliminowania przyczyny zdarzenia incydentu;
    3) działanie zapobiegawcze– działanie, które należy przedsięwziąć aby w przyszłości ograniczyć lub wyeliminować przyczyny zaistniałego zdarzenia/ incydentu.
8. Postępowanie z zaistniałym lub potencjalnie istniejącym incydentem wywołanym przez określone zagrożenia, odbywa się zgodnie z podejściem *risk based approach* opisanym w procedurze zarządzania ryzykiem (w załączniku do Polityki Ochrony Danych).
9. Rejestr incydentów znajduje się w załączniku do Polityki Ochrony Danych.
10. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii– ze względu na swój charakter, zakres, kontekst i cele- z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator **przed rozpoczęciem przetwarzania** dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
11. W przypadku kiedy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane

dotyczą, o takim naruszeniu.

12. Przez naruszenie praw lub wolności osoby fizycznej rozumie się:
    1) powstanie uszczerbku fizycznego, szkód majątkowych lub niemajątkowych takich jak utrata kontroli nad własnymi danymi osobowymi,
    2) ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości,
    3) stratę finansową, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia,
    4) naruszenie poufności danych osobowych chronionych tajemnicą zawodową,
    5) wszelkie inne znaczące szkody gospodarcze lub społeczne.
13. Administrator systemów informatycznych prowadzi dziennik zdarzeń/ incydentów (załącznik do Polityki Ochrony Danych).

POSTANOWIENIA KOŃCOWE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków służbowych, w szczególności przez osobę, która po stwierdzeniu naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie bezpośredniego przełożonego i zgodnie z wewnętrzną procedurą.
2. 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 kiedy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie.
3. Orzeczona kara wobec osoby uchylającej się od powiadomienia j.w. nie wyklucza odpowiedzialności karnej oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego o zrekompensowanie poniesionych strat.
4. Wdrożenie Polityki Ochrony Danych oraz działania korygujące i zachowawcze odbywają się poprzez:
    1) Zapoznanie osób uprawnionych do przetwarzania danych osobowych z treścią Polityki Ochrony Danych;
    2) Okresowe szkolenia z zakresu ochrony danych osobowych.
5. Polityka Ochrony Danych wchodzi w życie z dniem podpisania jej przez Administratora.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Podstawowe definicje

Ilekroć w instrukcji jest mowa o:

1. Polityce Ochrony Danych- rozumie się przez to politykę ochrony danych w Hemoklinika Sp. z o.o. ul. Stanisławy Leszczyńskiej 18 lok. 2; 93-347 Łódź zwanym dalej **Hemoklinika** lub **Administrator**.
2. Instrukcji– rozumie się przez to instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3. Systemie informatycznym- rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną Administratora.
4. Programie- rozumie się przez to program komputerowy wykorzystywany do pracy na danej jednostce komputerowej przez użytkownika.
5. Pozostałe pojęcia i skróty opisane są w pkt I Polityki Ochrony Danych.

Wprowadzenie

1. Instrukcja Zarządzania Systemem Informatycznym, zwana dalej w treści **Instrukcja**, została sporządzona w oparciu o art. 32 ust.1 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.
2. Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, a w szczególności: sposób rejestrowania i wyrejestrowania użytkownika, sposób przydziału haseł i zasady korzystania z nich, procedury rozpoczęcia i zakończenie pracy, obowiązki użytkownika, metodę i częstotliwość tworzenia kopii, zasady sprawdzania obecności wirusów komputerowych oraz dokonywania przeglądów i konserwacji systemu.
3. System informatyczny tworzą obecne i przyszłe serwery, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe, a także inne urządzenia stanowiące elementy systemu informatycznego lub połączone z systemem informatycznym.
4. Systemy zlokalizowane są zgodnie z opisem zawartym w Polityce Ochrony Danych

§ 1.

Ogólne zasady zabezpieczenia sprzętu informatycznego, danych i oprogramowania

1. Kontroli podlega dostęp do pomieszczeń, w których znajduje się sprzęt komputerowy, w celu zabezpieczenia sprzętu oraz danych osobowych i oprogramowania przed ich wykorzystaniem lub zniszczeniem przez osoby trzecie.
2. Wszystkie pomieszczenia, które należą do obszaru przetwarzania danych, wyposażone są w zamknięcia. W czasie, gdy nie znajdują się w nich osoby upoważnione, pomieszczenia są zamykane w sposób uniemożliwiający wstęp osobom nieupoważnionym. Osoby nieupoważnione mogą przebywać w obszarze przetwarzania danych tylko w obecności osób upoważnionych.
3. Wszystkich pracowników obowiązuje bezwzględny zakaz wynoszenia z **Hemokliniki** nośników z oprogramowaniem lub innymi danymi, chyba że zgodę na taką czynność wyrazi Administrator lub powołany przez niego Administrator Systemów Informatycznych
4. Na stanowiskach pracy, na których przetwarzane są dane osobowe, ekrany monitorów powinny być ustawione w sposób uniemożliwiający osobom trzecim wgląd w wyświetlane informacje.

§ 2.

Nadawanie uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych.
2. Użytkownikiem systemu informatycznego (osobą upoważnioną) może być:
   1) osoba zatrudniona przy przetwarzaniu danych osobowych, która posiada upoważnienie do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład;
   2) przedstawiciel innego podmiotu lub przedsiębiorca będący osobą fizyczną prowadzący działalność na podstawie wpisu do ewidencji działalności gospodarczej, którzy świadczą na podstawie stosowanych umów usługi związane z ich pracą w systemie informatycznym (serwis, zlecenie przetwarzania danych osobowych itp.).
3. Uzyskanie uprawnień następuje na dwóch poziomach:
   1) zarejestrowania w sieci komputerowej (założenie konta),
   2) nadanie określonych uprawnień do korzystania z systemu informatycznego.
4. Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.
5. Upoważnienie nadaje i odwołuje Administrator lub osoba działająca w jego imieniu.

6. Przed nadaniem upoważnienia Administrator sprawdza czy osoba upoważniona:
   1) odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych;
   2) podpisała oświadczenie o zachowaniu poufności;
   3) będzie przetwarzać dane osobowe w zakresie i celu zgodnym z Polityką Ochrony Danych i Instrukcją Zarządzania Systemem Informatycznym.
7. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik do Polityki Ochrony Danych.
8. Identyfikator użytkownika, po wyrejestrowania z systemu, nie może być przekazywany innej osobie.
9. Upoważnienia do przetwarzania danych osobowych rejestrowane są w ewidencji osób upoważnionych do przetwarzania danych osobowych (załącznik do Polityki Ochrony Danych). Ewidencję prowadzi Administrator

§ 3.

Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem.
2. Każdorazowe uwierzytelnienie użytkownika w systemie następuje po podaniu loginu i hasła.
3. Używanie hasła jest obowiązkowe dla każdego użytkownika, posiadającego login w systemie.
4. Obowiązują następujące zasady tworzenia hasła:
   1) administrator lub powołany przez niego ASI nadaje każdemu użytkownikowi unikalny identyfikator i hasło ze wskazaniem dostępnego zakresu danych i operacji;
   2) hasło pierwszego logowania ustala Administrator lub powołany przez niego ASI. Każdy użytkownik systemu informatycznego ma obowiązek dokonać jego zmiany na indywidualne hasło;
   3) hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów;
   4) hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne: (A-Z) – duże litery alfabetu; (a-z) – małe litery alfabetu; (0-9) – cyfry; (!, @, #, $, %,...,) - znaki specjalne;
   5) hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury;
   6) hasło nie może być jednakowe z identyfikatorem użytkownika;
   7) hasło musi być unikalne, czyli takie, które nie było poprzednio stosowane przez użytkownika;
   8) loginy i hasła umożliwiające dostęp do komputerów posiada Administrator.
5. Obowiązują następujące zasady korzystania z haseł:
   1) zabrania się ujawniania haseł jakimkolwiek osobom trzecim,
   2) zabrania się zapisywania haseł lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim.
6. Hasło, w trakcie jego wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
7. Hasło musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.
8. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie Administratora.
9. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, jest niezwłocznie zablokowany w systemie informatycznym służącym do przetwarzania danych osobowych, a przypisane mu hasło unieważnione.

§ 4.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić

urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych. W przypadku naruszenia ochrony danych osobowych użytkownik niezwłocznie powiadamia Administratora lub powołanego przez niego ASI

2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
   1) włączenia stacji roboczej,
   2) uwierzytelnienia się („zalogowania" w systemie) za pomocą loginu i hasła.
3. Niedopuszczalne jest uwierzytelnianie się na hasło i login innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.
4. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się" z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności dyskietki, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.
5. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się" lub zaktywizować wygaszacz ekranu z opcją ponownego „logowania" się do systemu.
6. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się" w systemie), użytkownik niezwłocznie powiadamia o nich Administratora.
7. Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników.

§ 5.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania

1. Kopią zapasową i awaryjną objęte są dane znajdujące się na stacjach roboczych posiadających lokalnie zainstalowane systemy.
2. Kopie danych zawartych w systemie należy tworzyć każdorazowo po zakończeniu dnia pracy oraz w cyklu tygodniowym, miesięcznym i rocznym.
3. Kopie są okresowo, raz w miesiącu, sprawdzane pod kątem ich przydatności do odtworzenia danych, a jeżeli ustanie ich użyteczność są niezwłocznie usuwane.
4. Za sporządzenie i bezpieczeństwo kopii zapasowych oraz awaryjnych odpowiedzialny jest Administrator lub wyznaczony przez niego ASI, który po ich sporządzeniu zabezpiecza je w pomieszczeniu przetwarzania danych osobowych. Każda następna kopia zapisywana jest w miejsce poprzedniej.
5. Kopie należy wykonać na nośniku wymienialnym na stacji posiadającej dostęp do danych.
6. Należy sporządzać kopie przez przegrywanie całej bazy danych.
7. Należy sprawdzać kopie awaryjne pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu- co najmniej jednorazowo po przegraniu danych. Kopie awaryjne należy bezzwłocznie usuwać po ustaniu ich użyteczności.
8. Należy tworzyć kopie awaryjne przed każdą aktualizacją systemu informatycznego, składników systemu informatycznego lub poszczególnych programów służących do przesyłania lub przetwarzania danych, w szczególności:
   1) przed wprowadzeniem nowej wersji oprogramowania,
   2) przed reinstalacją systemu operacyjnego
   3) przed naprawą serwera lub urządzenia pełniącego jego rolę
   4) przed wykonaniem niestandardowych czynności związanych z bazą danych (np. uruchomienie oprogramowania sprawdzającego lub przywracającego integralność bazy danych),
9. Harmonogram sporządzania kopii zapasowych musi gwarantować dostępność w każdej chwili kopii z ostatniego dnia, z końca ubiegłego tygodnia i ubiegłego roku.
10. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych należy przechowywać w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
11. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopii zapasowych systemów informatycznych służących do przetwarzania danych osobowych mają one zostać uszkodzone w sposób uniemożliwiający odczyt danych osobowych.

§ 6.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Wydruki i dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w odrębnych zamykanych szafach.
2. Osoba zatrudniona przy przetwarzaniu danych osobowych sporządzająca wydruk zawierający dane osobowe ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności– niezwłocznie wydruk zniszczyć.
3. Elektroniczne nośniki informacji z danymi osobowymi są oznaczane i przechowywane w zamykanych szafach lub sejfach znajdujących się w specjalnym pomieszczeniu, do którego dostęp mają wyłącznie odrębnie upoważnieni pracownicy.
4. Fizyczna likwidacja zniszczonych lub niepotrzebnych elektronicznych nośników informacji z danymi osobowymi odbywa się w sposób uniemożliwiający odczyt danych osobowych.
5. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.
6. Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe są kasowane lub zniszczone tak, aby nie było możliwe ich odczytanie. Należy przy tym stosować następujące zasady:
   1) kopie zapasowe należy przechowywać w systemie dziennym przez okres roku. Po tym okresie dane mogą być usunięte w sposób ręczny z pozostawieniem kopii rocznej.
   2) usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
   3) w przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika– odpowiedzialny za ich zniszczenie jest użytkownik.
   4) przez zniszczenie nośników informacji rozumie się ich trwałe i nieodwracalne zniszczenie do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.
7. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe zapisane na nośnikach oraz wydruki i inne dokumenty zawierające dane osobowe należy przechowywać w pomieszczeniach określonych w Polityce Ochrony Danych w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.
8. W przypadku uszkodzenia lub zużycia nośnika informacji zawierającego dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.
9. Urządzenia, dyski lub inne nośniki informacji przeznaczone do:
   1) likwidacji- należy pozbawić danych poprzez formatowanie oraz fizyczne uszkodzenie, uniemożliwiające ich odczytanie,
   2) przekazania- należy pozbawić zapisu zawierającego dane osobowe,
   3) naprawy- należy pozbawić zapisu danych osobowych lub naprawić pod nadzorem osoby do tego upoważnionej przez Administratora.

§ 7.

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Przyłączenia sieci internetowej do systemu, w którym przetwarzane są dane osobowe odbywa się pod następującymi warunkami:
   1) na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe;
   2) każdy e-mail wpływający do systemu musi być sprawdzony pod kątem występowania wirusów;
   3) aktualizacje programów antywirusowych muszą być dokonywane nie rzadziej niż raz w tygodniu;
   4) zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym, którego dokonuje użytkownik zamierzający go użyć;

5) zabrania się pobierania z Internetu plików niewiadomego pochodzenia oraz odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym;
6) zabrania się użytkownikom stacji roboczych wyłączania, blokowania, odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem;
7) zabrania się ściągania na stacje robocze i nośniki danych i oprogramowania z Internetu;
8) zabrania się nieautoryzowanego instalowania własnego oprogramowania na służbowych stacjach roboczych.

2. Po każdej naprawie i konserwacji stacji roboczej należy dokonać jej sprawdzenia pod kątem występowania wirusów i ponownie zainstalować program antywirusowy.
3. Elektroniczne nośniki informacji pochodzenia zewnętrznego, przed rozpoczęciem korzystania z nich, podlegają sprawdzeniu programem antywirusowym. Dane uzyskiwane drogą teletransmisji należy umieszczać, przed ich otwarciem, w katalogu przejściowym, który podlega sprawdzeniu.
4. Użytkownicy systemu są odpowiedzialni za nieudostępnianie stanowisk pracy osobom postronnym nieuprawnionym do dostępu do systemu informatycznego, w którym przetwarza się dane osobowe.
5. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 8.

Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

1. Dane osobowe mogą być wydane jedynie na wniosek osoby, której dotyczą lub wniosek osoby upoważnionej przez zainteresowanego.
2. W systemie informatycznym służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia.
3. W przypadku, gdy w systemie informatycznym służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, Administrator lub wskazana przez niego osoba odnotowuje je w zestawieniu udostępnianych danych osobowych. W zestawieniu odnotowywane są imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia. Wzór zestawienia stanowi załącznik w Polityce Ochrony Danych.

§ 9.

Wykonywanie przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w Polityce Ochrony Danych.
2. Procedury naprawy sprzętu komputerowego:
   1) naprawa sprzętu komputerowego użytkowanego w systemie może odbywać się w siedzibie Administratora i dokonywać jej może jedynie wyspecjalizowaną firma lub osoba. Czynności te muszą być wykonywane w obecności osoby upoważnionej przez Administratora.
   2) przed naprawą sprzętu komputerowego użytkowanego w systemie poza siedzibą Administratora należy usunąć z twardego dysku wszelkie aplikacje przetwarzające i zawierające dane o charakterze osobowym. Administrator jest odpowiedzialny za stworzenie kopii tej bazy i przechowywanie jej w bezpiecznym miejscu.
   3) po powrocie z serwisu sprzętu komputerowego Administrator lub upoważniona przez niego osoba ponownie instaluje bazę danych, a jej kopia zostaje zniszczona.
3. Procedura przeglądu systemu:

1) przegląd systemu dokonuje osoba obsługująca go względem informatycznym, która została do tego upoważniona przez Administratora
2) czynności przeglądowe dokonywane przez osobę zewnętrzną obsługującą Administratora pod względem informatycznym mają być przeprowadzone w obecności pracownika upoważnionego przez Administratora.
3) zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji może być dokonana tylko za wiedzą i zgodą Administratora.
4) przeglądy techniczne muszą być dokonywane nie rzadziej niż raz w roku.

§ 10.

Sposoby postępowania w zakresie komunikacji w sieci informatycznej

1. Wszelkie pliki zawierające kopie danych osobowych zawartych w systemie, wysyłanych poza system, muszą być zabezpieczone hasłem.
2. W miarę możliwości, dane osobowe zawarte na serwerze sieciowym nie mogą być przechowywane na stacjach roboczych. Należy je umieszczać na dysku sieciowym.
3. Nieuzasadnione kopiowanie danych z serwera (lub urządzenia pełniącego jego funkcje) na stacje robocze bądź na nośniki informatyczne jest zabronione.

§ 11.

Zasady korzystania z urządzeń przenośnych do przetwarzania danych osobowych

1. Osoba użytkująca przenośne urządzenie, służące do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas jego transportu i przechowywania poza obszarem, przeznaczonym do przetwarzania danych osobowych.
2. W celu zapobieżenia dostępowi do tych danych osobie niepowołanej, należy:
   1) zabezpieczyć dostęp do urządzenia i systemu operacyjnego poprzez identyfikator i hasło;
   2) nie zezwalać na używanie urządzenia osobom nieupoważnionym do dostępu do danych osobowych.
3. Należy zachować wyjątkową ostrożność:
   1) przy przetwarzaniu danych osobowych w obszarach użyteczności publicznej;
   2) przy podłączeniu do sieci publicznych poza obszarem przetwarzania danych osobowych.

§ 12.

Postanowienia końcowe

1. Niniejsza Instrukcja jest zgodna z postanowieniami powszechnie obowiązującego prawa.
2. Użytkownik systemu jest zobowiązany zapoznać się z treścią niniejszej Instrukcji i potwierdzić to stosownym oświadczeniem.
3. Naruszenie przez osobę postanowień niniejszej Instrukcji może zostać potraktowane jako naruszenie obowiązków służbowych i powodować, określoną stosownymi przepisami, odpowiedzialność tej osoby.
4. Treść niniejszej Instrukcji ma charakter poufny, chroniony tajemnicą pracodawcy na zasadzie art. 100 § 2 pkt 4 Kodeksu Pracy oraz innych przepisów.
5. W sprawach nieunormowanych stosuje się przepisy Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000) oraz 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 (Dz. Urz. UE L 119 z 04.05.2016, s. 1).

ZAŁĄCZNIKI

Spis załączników

1.	Załącznik nr 1	Rejestr czynności przetwarzania
2.	Załącznik nr 2	Wykaz budynków i pomieszczeń, w których są przetwarzane dane osobowe
3.	Załącznik nr 3	Oświadczenie osoby upoważnionej do przetwarzania danych osobowych
4.	Załącznik nr 4	Upoważnienie imienne do przetwarzania danych osobowych
5.	Załącznik nr 5	Ewidencja osób upoważnionych do przetwarzania danych osobowych
6.	Załącznik nr 6	Rejestr udostępnień danych osobowych
7.	Załącznik nr 7	Zestawienie przekazywanych danych osobowych
8.	Załącznik nr 8	Wykaz umów powierzenia przetwarzania danych osobowych
9.	Załącznik nr 9	Lista uczestników szkolenia z ochrony danych osobowych
10.	Załącznik nr 10	Zarządzanie ryzykiem ochrony danych osobowych- procedura
11.	Załącznik nr 11	Zarządzanie ryzykiem ochrony danych osobowych- tabele
12.	Załącznik nr 12	Raport z incydentu
13.	Załącznik nr 13	Rejestr incydentów
14.	Załącznik nr 14	Ocena skutków ochrony danych DPIA- *Data Protection Impact Assesment*
15.	Załącznik nr 15	Dziennik zdarzeń Administratora Systemów Informatycznych

Załącznik nr 1 do Polityki Ochrony Danych

Rejestr czynności przetwarzania

(prowadzony w arkuszu kalkulacyjnym Excel)

Uwaga: Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. RODO jest zawarty w Polityce Ochrony Danych i Instrukcji Zarządzania Systemem Informatycznym

Załącznik nr 2 do Polityki Ochrony Danych

Wykaz budynków i pomieszczeń

Dane osobowe przetwarzane są w budynku mieszczącym się przy ul. Stanisławy Leszczyńskiej 18 lok. 2

93-347 Łódź

Lp.	Nr pomieszczenia	Przeznaczenie pomieszczenia	Rodzaj zabezpieczenia fizycznego
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			

Załącznik nr 3/…. do Polityki Ochrony Danych

Oświadczenie osoby upoważnionej do przetwarzania danych osobowych w Hemoklinika Sp. z o.o.

Imię i nazwisko……..

Łódź, dnia.....

Stanowisko ……..

OŚWIADCZENIE

Oświadczam, że przed przystąpieniem do pracy przy przetwarzaniu danych osobowych:

1. Zostałam(em) zaznajomiona(y) z rozporządzeniem 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) (Dz. Urz. UE L 119 z 04.05.2016, s. 1), ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000) oraz aktami wykonawczymi do w/w aktów prawnych
2. Znana jest mi odpowiedzialność karna za naruszenie ww. aktów prawnych.
3. Zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w Polityce Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym, a także w innych dokumentach regulujących zasady przetwarzania danych osobowych i zobowiązuję się do ich przestrzegania.
4. Zobowiązuję się:
    1. zachować w tajemnicy dane osobowe, z którymi zetknęłam się / zetknąłem się w trakcie wykonywania swoich obowiązków służbowych, zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu;
    2. chronić dane osobowe przed dostępem do nich osób do tego nieupoważnionych, zabezpieczać je przed zniszczeniem i nielegalnym ujawnieniem.

……

podpis

Załącznik nr 4 do Polityki Ochrony Danych Łódź, dnia .....

Upoważnienie imienne do przetwarzania danych osobowych[1]

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 upoważniam Panią(a)

……

zatrudnioną(ego) w Hemoklinika Sp. z o.o.

na stanowisku .....

do przetwarzania od dnia ..... danych osobowych w zakresie:

Lp.	Rodzaj dokumentacji tradycyjnej
1.	
2.	

Lp.	Aplikacje elektroniczne	Moduły	Poziom uprawnień (do zapisu/odczytu/modyfikacji/usuwania)
1.			
2.			
3.	Lokalne i sieciowe zasoby komputera		

i nadaję identyfikator[2] **……** (dla wersji elektronicznej).

..... ……

(podpis w imieniu Administratora) (podpis upoważnionej osoby)

[1] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)

[2] *Poinfomowano o obowiązku wprowadzenia hasła i pouczono o obowiązku ich zmiany*

Załącznik nr 4.1 do Polityki Ochrony Danych

Odwołanie upoważnienia imiennego do przetwarzania danych osobowych

w Hemoklinika Sp. z o.o. [3]

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 odwołuję upoważnienie Pani(a)

……..zatrudnionej(ego)

w Hemoklinika Sp. z o.o. na stanowisku ……

do przetwarzania od dnia …….. danych osobowych w zakresie:

Lp.	Rodzaj dokumentacji tradycyjnej
1.	
2.	

cofam prawo do korzystania z identyfikatora .....(dotyczy tylko

wersji elektronicznej).

Lp.	Aplikacje elektroniczne	Moduły	Poziom uprawnień (do zapisu/odczytu/modyfikacji/usuwania)
1.			
2.			
3.	Lokalne i sieciowe zasoby komputera		

..... ……

(podpis w imieniu Administratora) (podpis osoby upoważnionej)

Potwierdzam otrzymanie kopii niniejszego upoważnienia

……

(podpis osoby upoważnionej)

[3] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)

Załącznik nr 5 do Polityki Ochrony Danych

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Hemoklinika Sp. z o.o. [4]

Lp.	Imię i nazwisko użytkownika	Identyfikator użytkownika przy wersji elektronicznej	Zakres uprawnień	Data nadania uprawnień	Data odebrania uprawnień	Przyczyna odebrania uprawnień

[4] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)

Załącznik nr 6 do Polityki Ochrony Danych

Rejestr udostępnień dokumentacji medycznej pacjentowi

lub osobie przez niego upoważnionej[5]

L.p.	Nazwisko i imię, PESEL	Zakres udostępnienia	Sposób udostępnienia	Osoba udostępniająca (data i podpis)

[5] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)

Załącznik nr 7 do Polityki Ochrony Danych

Zestawienie przekazywanych danych osobowych[6]

Lp.	Imię i nazwisko/nazwa odbiorcy danych osobowych (komu przekazano dane)	Data przekazania danych osobowych	Opis osoby lub przekazanego zbioru (jakie dane zostały przekazane)	Podstawa prawna/numer umowy	Rodzaj zbioru/ zasobu (wydruk papierowy, elektroniczny, zdjęcie)	Osoba udostępniająca (data i podpis)
1.						
2.						
3.						
4.						
5.						
6.						
7.						

[6] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)

Załącznik nr 8 do Polityki Ochrony Danych

Wykaz umów powierzenia przetwarzania danych osobowych[7]

Lp.	Nazwa podmiotu, któremu powierzono dane	Okres powierzenia	Cel powierzenia	Rodzaj powierzonych danych	Czy są zapisy w umowie związane z poufnością i odpowiedzialnością w stosunku do powierzonych danych?
1.					
2.					
3.					
4.					
5.					
6.					
7.					

[7] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)

Załącznik nr 9 do Polityki Ochrony Danych

Lista uczestników szkolenia z ochrony danych osobowych[8]

Data szkolenia: ……

Miejsce szkolenia:……..

Zakres szkolenia: ……

……

Osoba prowadząca: …….

Lp.	Imię i nazwisko uczestnika	Stanowisko	Podpis	Uwagi
1.				
2.				
3.				
4.				

[8] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)

5.				
6.				
7.				
8.				
9.				
10.				

Załącznik nr 10 do Polityki Ochrony Danych

Zarządzanie ryzykiem ochrony danych osobowych- procedura

Pojęcie ryzyka

1. Ryzyko w ochronie danych osobowych w podmiocie wykonującym świadczenia lecznicze to negatywny wpływ jaki wywierają różne zagrożenia na prawa i wolności osób, których dane są przetwarzane. Osobami tymi są w szczególności:
   1) Pacjenci
   2) Opiekunowie prawni
   3) Osoby upoważnione przez pacjenta
   4) Personel
   5) Kontrahenci
   6) Kandydaci do pracy
2. Ryzyko w ochronie danych osobowych jest określane poprzez kombinację skutku i prawdopodobieństwa zaistnienia w przyszłości niekorzystnych zdarzeń związanych z ochroną tych danych. Jest to prawdopodobieństwo tego, że zagrożenia się zrealizują i przyniosą konkretny, negatywny skutek dla posiadanych zasobów. Jest to w szczególności:
   1) Ryzyko utraty poufności danych skutkujące naruszeniem praw lub wolności osób, których te dane dotyczą
   2) Ryzyko utraty dostępu do zasobów powodujące naruszenie ciągłości działania (ryzyko ciągłości działania)
   3) Ryzyko prawne związane z:
      a. możliwym niedopasowaniem się do przepisów regulujących ochronę danych osobowych
      b. roszczeniami osób, których dane osobowe (w tym medyczne) są przetwarzane
      c. roszczeniami stron kontraktów w przypadku braku możliwości wywiązanie się z zawartych umów
   4) Ryzyko niematerialne – utrata reputacji
   5) Ryzyko finansowe związane z ograniczonymi możliwościami zabezpieczenia się przed stratami finansowymi
3. Oszacowanie ryzyka zmniejsza niepewność *sensu stricto*[1] i jest podstawą podjęcia decyzji o dalszym postępowaniu z ryzykiem

Zarządzanie ryzykiem w ochronie danych osobowych

1. Zarządzanie ryzykiem to proces, który polega na wyszukiwaniu potencjalnych zagrożeń i ograniczania skutków oraz prawdopodobieństwa zdarzeń, które mogą powstać z powodu tych zagrożeń. Obejmuje specyficzne działania, których celem jest uniknięcie lub minimalizowanie prawdopodobieństwa i skutków wystąpienia zagrożeń w ochronie danych osobowych.
2. Podstawą zarzadzania ryzykiem jest przewidywanie:
   1) Procesów przetwarzania danych osobowych w kontekście posiadanych zasobów
   2) Ponoszonych w tym zakresie kosztów
   3) Jakości procesu udzielania świadczeń leczniczych

Etapy zarządzania ryzykiem

1. W celu utrzymania i doskonalenia procesu zarządzania ryzykiem w ochronie danych osobowych wprowadza się następujące etapy zarządzania ryzykiem:
    1) Ustalenie kontekstu. polegające na ocenie:
        a. warunków instytucjonalnych,
        b. zbiorów danych oraz przepływu danych
        c. stosowanych zabezpieczeń
        d. poziomu akceptowalnego ryzyka (ryzyko rezydualne);
        e. przyjętych środków kontroli
    2) Szacowanie ryzyka, które obejmuje:
        a. identyfikację zagrożeń w odniesieniu do określonych zasobów
        b. analizę skutków i prawdopodobieństwa wystąpienia niekorzystnych zdarzeń wywołanych przez dane zagrożenia
        c. określenie poziomów ryzyka;
    3) Postępowanie z ryzykiem. zyli podjęcie decyzji co do wyboru działań:
        a. redukcji ryzyka
        b. akceptacji ryzyka
        c. unikania ryzyka
        d. przeniesienia ryzyka;
    4) Wdrożenie postępowania według opracowanego planu
    5) Monitorowanie ryzyka
2. Podczas szacowania ryzyka Administrator:
    1) Identyfikuje zagrożenia w odniesieniu do zasobów (zgodnie z Tabelą A):
        a. fizycznych- dotyczących zabezpieczeń i stref ochronnych lokalizacji, budynków i obszarów przetwarzania danych osobowych
        b. technologicznych- związanych z utrzymaniem określonej infrastruktury, aplikacji
        c. organizacyjnych, którymi są polityki bezpieczeństwa, procedury i regulaminy
        d. personalnych, czyli kwalifikacji i standardów zachowań osób uprawnionych do przetwarzania danych osobowych
    2) Analizuje skutki (S) zgodnie z tabela punktową skutków oddziaływania (Tabela B)
    3) Analizuje prawdopodobieństwo (P) wystąpienia niepożądanych zdarzeń zgodnie z tabelą C
    4) Oblicza wartość punktową ryzyka R według wzoru R= P x S, a wyniki zamieszcza w kolumnie 5 w tabeli D
    5) Przypisuje wartość punktową ryzyka do odpowiedniego poziomu ryzyka zgodnie z załącznikiem E. Wynik zamieszcza w kolumnie 6 w załączniku D
    6) Wdraża określone postępowanie zgodnie z punktem 2. 3 oraz opisem w załączniku E

Postanowienia końcowe

1. Szacowanie ryzyko jest na bieżąco dokumentowane
2. Procedura zarządzania ryzykiem podlega raz w roku przeglądowi w celu jej aktualizacji
3. Administrator szacuje ryzyka:
    1) Przynajmniej raz w roku
    2) Częściej, jeśli zachodzi taka konieczność
    3) Przy każdej ocenie skutków dla ochrony danych zgodnie z art. 35 RODO

Załącznik nr 11/……. do Polityki Ochrony Danych

Zarządzanie ryzykiem ochrony danych osobowych - tabele[9]

Tabela A: Identyfikacja zagrożeń

Lp.	Rodzaj zasobu (O/T/F/P)[10]	Opis potencjalnych zagrożeń
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

[9] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)
[10] O- organizacyjne; T- techniczne; F- fizyczne; P- personalne

Lp.	Rodzaj zasobu (O/T/F/P)[10]	Opis potencjalnych zagrożeń
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		

Tabela B: Analiza skutków oddziaływania (S)

Opis	Punktacja	Skutki oddziaływania na Administratora	Skutki dla osoby fizycznej, której dane są przetwarzane
Bardzo wysoki	5	Poważne straty finansowe, brak możliwości realizacji kluczowych zadań. Poważny incydent. Informacje w mediach ogólnopolskich	Trwała niezdolność do pracy, głębokie zadłużenie, utrata majątku lub większości dóbr materialnych, śmierć trwałe kalectwo, ubezwłasnowolnienie, utrata więzi rodzinnych, utrata dostępu do prądu, wody
Wysoki	4	Istotne straty finansowe. Duże zakłócenia w gospodarowaniu danymi osobowymi. Wysoki incydent. Pewne informacje w mediach lokalnych lub regionalnych	Pogorszenie sytuacji majątkowej, utrata pracy, trafienie na czarną listę instytucji (wykluczenie przez instytucję) , dolegliwości psychiczne (depresja, fobia), skutki sądowe
Średni	3	Średnie straty finansowe. Niewielkie zakłócenia w gospodarowaniu danymi osobowymi. Średni incydent. Ograniczone informacje w mediach lokalnych lub regionalnych	Dodatkowe koszty, przerwa w dostępie do usług, danych, krótkotrwały stres, strach, problemy w relacjach, niewielkie dolegliwości psychiczne, dezinformacja, dezorientacja
Niski	2	Niskie straty finansowe. Małe zakłócenia w gospodarowaniu danymi osobowymi. Drobny incydent. Brak informacji lub jednorazowa informacje w mediach lokalnych lub regionalnych	Konieczność uzupełnienia danych, irytacja, poczucie zagrożenia, utrata czasu
Bardzo niski	1	Nieznaczne straty finansowe. Nieistotne zakłócenia w gospodarowaniu danymi osobowymi. Nieistotny incydent. Brak informacji w mediach lokalnych lub regionalnych	Chwilowa irytacja, strach nad utratą kontroli nad własnymi danymi osobowymi

Uwagi: Analiza skutków oddziaływania (S) niekorzystnych zdarzeń dokonywana jest w oparciu o następujące kryteria:

1) Dostępność, poufność i rozliczalność przetwarzanych danych osobowych
2) Pogorszenie funkcjonalności przetwarzania danych osobowych
3) Straty finansowe
4) Zakłócenia w udzielaniu świadczeń leczniczych
5) Wymagania prawne oraz zobowiązania umowne
6) Następstwa dla wizerunku i reputacji

Tabela C: Analiza prawdopodobieństwa wystąpienia zdarzenia

Prawdopodobieństwo	0-10%	11-30%	31%-50%	51-70%	71-100%
Poziom	Rzadkie	Mało prawdopodobne	Możliwe	Prawdopodobne	Prawie pewne
Punktacja	1	2	3	4	5
Opis	Minimalna szansa na wystąpienie zagrożenia	Zagrożenie nie występuje lub występuje okazjonalnie	Zagrożenie nie wystąpiło w podmiocie w ostatnim okresie, ale wystąpiło w innych podmiotach	Zagrożenie jest realne, miało miejsce w podmiocie	Zagrożenie jest wysokie, często występuje w trakcie realizowanych zadań

Uwagi: Analiza prawdopodobieństwa wystąpienia niepożądanych zdarzeń (P) uwzględnia następujące kryteria:

1) Statystyki dotyczące podobnych zdarzeń,
2) Atrakcyjność danego zasobu,
3) Czynniki środowiskowe,
4) Rodzaj zagrożenia powodującego incydent,
5) Istniejące zabezpieczenia.

Tabela D: Obliczenie wartości ryzyka[11]

1.	2.	3.	4.	5.	6.
Lp.	**Opis potencjalnych zagrożeń**	**Prawdopodobieństwo** wystąpienia zagrożenia w	**Skutek oddziaływania** zagrożenia w skali 1-5	**Wartość ryzyka** iloczyn skutku i prawdopodobieństwa. (5 = 3 x 4)	**Poziom ryzyka** w skali 1-4
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

[11] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)

1.	2.	3.	4.	5.	6.
Lp.	**Opis potencjalnych zagrożeń**	**Prawdopodobieństwo** wystąpienia zagrożenia w	**Skutek oddziaływania** zagrożenia w skali 1-5	**Wartość ryzyka** iloczyn skutku i prawdopodobieństwa. (5 = 3 x 4)	**Poziom ryzyka** w skali 1-4
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					

Tabela E: Poziom ryzyka (w skali 1-4)

Poziom ryzyka	Skala	Opis działania
Niski (N)	1	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów
Średni (Ś)	2	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga **okresowego** monitorowania
Wysoki (W)	3	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga **stałego** monitorowania
Krytyczny (K)	4	Poziom ryzyka nietolerowany – wymaga **natychmiastowego działania**

Uwaga: Wartości ryzyka są przedstawione na poniższej mapie ryzyka

MAPA RYZYKA

			SKUTEK				
			Bardzo niski	**Niski**	**Średni**	**Wysoki**	**Bardzo wysoki**
			1	2	3	4	5
PRAWDOPODOBIEŃSTWO	**Prawie pewne**	5	Ś (5)	W (10)	K (15)	K (20)	K (25)
	Prawdopodobne	4	Ś (4)	W (8)	W (12)	K (16)	K (20)
	Możliwe	3	N (3)	Ś (6)	W (9)	W (12)	K (15)
	Mało prawdopodobne	2	N (2)	Ś (4)	Ś (6)	W (8)	W (10)
	Rzadkie	1	N (1)	N (2)	Ś (3)	W (4)	W (5)

Załącznik nr 12 do Polityki Ochrony Danych

Raport z incydentu naruszającego bezpieczeństwo danych osobowych[12]

1. Data i godzina otrzymania informacji o naruszeniu:

……

……

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……

……

3. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:

……

……

[12] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)

4. Informacje o danych, które zostały lub mogły zostać ujawnione:

……

……

5. Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

……

……

6. Opis zdarzenia związanego z naruszeniem ochrony danych osobowych:

……

……

……

7. Ocena skutków działań niepożądanych będących następstwem incydentu:

……

……

8. Określenie wagi incydentu zgodnie z procedurą oceny skutków (DPIA)

……

……

9. Wdrożenie działań naprawczych

……

……

……

……

……

10. Ocena konieczności powiadomienia organu nadzoru i osób których te dane dotyczą

……

……

11. Wykaz załączników do raportu

……

……

12. Data raportu i osoba sporządzająca raport

……

……

Załącznik nr 13 do Polityki Ochrony Danych

Rejestr incydentów[13]

Nr incydentu (zał. nr 15)	**Data i miejsce naruszenia**	**Osoba zgłaszająca naruszenie**	**Poziom ryzyka** (Wynik przeprowadzonej analizy ryzyka)	**Podjęte działania zaradcze**	**Zgłoszenie organowi nadzorczemu i osobie TAK/NIE**	**Status (w toku/ zakończone)**

[13] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)

Załącznik nr 14 do Polityki Ochrony Danych

Ocena skutków dla ochrony danych (DPIA)

Przesłanki stosowania oceny skutków dla ochrony danych

1. Ocena skutków dla ochrony danych - *DPIA – Data Protection Impact Assesment* – nałożony przez RODO obowiązek analizy w jaki sposób operacja przetwarzania danych osobowych (planowana a także już prowadzona) wpływa lub będzie wpływać na prawa i wolności osób, których dane są przetwarzane w ramach danej operacji przetwarzania.
2. Wymóg przeprowadzenia oceny skutków dla ochrony danych dotyczy:
   1) Istniejących operacji przetwarzania, które ze względu na użycie nowych technologii, zakres i kategorie przetwarzania mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, których dane są przetwarzane
   2) Zmiany rodzaju ryzyka, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania
3. Ocena skutków dla ochrony danych w praktyce przeprowadzana będzie dla wszelkich przedsięwzięć (np. projektów, zakupów urządzeń i nowych technologii) i procesów, podczas których przetwarzane są lub będą dane osobowe i z tym przetwarzaniem wiąże się ryzyko (obecnie lub w przyszłości) naruszenia praw i wolności osób fizycznych.
4. Administrator weryfikuje czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych. Konsultuje się w tym zakresie z powołanym przez niego IOD, lub w razie potrzeby z ekspertami, osobami, których te dane dotyczą lub z ich przedstawicielami

Naruszenie praw i wolności

1. Prawa osób, których dane są przetwarzane dotyczą w szczególności:
   1) Wolności słowa,
   2) Wolności myśli,
   3) Swobody przemieszczania się,
   4) Zakazu dyskryminacji,
   5) Wolności sumienia i religii
   6) Dysponowania swoimi danymi w zakresie i trybie przewidzianym w regulacji RODO oraz obowiązującymi na jej podstawie aktami wykonawczymi
2. Każda ocena wpływu na ochronę danych osobowych musi uwzględniać prawa i wolności odpowiednio do rozpatrywanej operacji przetwarzania danych osobowych
3. Ocena powinna uwzględniać wszelkie negatywne skutki, które mogą prowadzić do szkód fizycznych, materialnych i niematerialnych.

Odpowiedzialność za przeprowadzenie oceny skutków ochrony danych

1. Administrator ponosi odpowiedzialność za inicjatywę dokonania oceny oraz jej przeprowadzenie.
2. Administrator przy dokonywaniu oceny skutków może skorzystać z pomocy innych osób, nie zwalnia go to jednak z bezpośredniej odpowiedzialności za proces.

3. Administrator przy przeprowadzaniu DPIA ma obowiązek konsultowania się z powołanym przez niego Inspektorem Ochrony Danych.
4. Administrator może również zasięgnąć opinii w kwestii oceny skutków dla ochrony danych wśród osób, których dane osobowe są przetwarzane.
5. Wszelkie czynność związane z przeprowadzaniem DPIA lub oceną konieczności jej przeprowadzenia są pisemnie dokumentowane.
6. Jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym.
7. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Elementy oceny skutków ochrony danych

1. Systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym (gdy ma to zastosowanie) prawnie uzasadnionych interesów realizowanych przez Administratora.
2. Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów.
3. W odniesieniu do potencjalnego naruszenia praw i wolności osób fizycznych dokonywanie analizy ryzyka potencjalnych incydentów wraz ze środkami minimalizującymi to ryzyko oraz uzasadnieniem dokonanego wyboru środków.
4. Planowane środki mające na celu zaradzenie ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
5. W przypadku dokonanego naruszenia praw i wolności osób fizycznych przeprowadzenie analizy wagi incydentu połączonej z analizą przyczyn incydentu Dla każdej przyczyny należy określić środki zaradcze, które zminimalizują jego wystąpienie w przyszłości.
6. Uwzględnienie, przy obliczeniu wagi dokonanego incydentu, rodzaj danych osobowych, zakres naruszenia, czas oraz koszt odtworzenia systemu oraz konsekwencje prawne i wizerunkowe.

Publikowanie oceny skutków ochrony danych

1 Wyniki oceny skutków ochrony danych powinny zostać udostępnione publicznie jeżeli operacja przetwarzania ma duży wpływ na liczną grupę społeczną

2 Publikacji w ramach DPIA nie podlegają informacje poufne, w tym dotyczące stosowanych środków bezpieczeństwa.

Załącznik nr 15 do Polityki Ochrony Danych

Dziennik zdarzeń Administratora Systemów Informatycznych[14][15]

Lp.	Data incydentu/ zdarzenia	Rodzaj incydentu/ zdarzenia	Opis incydentu/ zdarzenia	Uwagi

[14] Dokument elektroniczny/ tradycyjny (niepotrzebne skreślić)
[15] Jeśli nie został powołany Administrator Systemów Informatycznych to jego obowiązki przejmuje inna osoba