Załącznik nr 2 do Regulaminu systemu

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

SYSTEMU ASYSTENT EFS

Celem Polityki Bezpieczeństwa Danych Osobowych w zbiorach manualnych oraz elektronicznych, (zwanej dalej Polityką Bezpieczeństwa), jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w tym 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 (RODO) i jego obowiązywaniem od 25 maja 2018 r., sposobu przetwarzania informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi jakie mogą zaistnieć w związku z korzystaniem przez użytkowników z strony www.asystentefs.pl oraz Systemu Asystent EFS, których operatorem jest Project Hub Sp. z o.o. z/s w Poznaniu.

§1 Definicje

1) **Administrator Danych Osobowych (Administrator)** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,.
2) **Dane osobowe** – oznaczają wszelkie 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.
3) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do
   pracy w systemie informatycznym Administratora;
4) **Odbiorca danych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
5) **Strona trzecia** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny
   niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które

z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe;

6) **Osoba upoważniona do przetwarzania danych osobowych (Osoba upoważniona)** – osoba,
   która została upoważniona do przetwarzania danych osobowych przez Administratora;
7) **Poufność danych** – rozumie się jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom i podmiotom,
8) **Dostępność danych** – rozumie się jako właściwość zapewniającą, że upoważnieni Użytkownicy
   mają dostęp do informacji w każdej sytuacji, kiedy jest to niezbędne do realizacji ich zadań;
9) **Integralność danych** – rozumie się jako właściwość zapewniającą, że dane nie zostały zmienione
   lub zniszczone w sposób nieautoryzowany;
10) **Postać elektroniczna danych** – dane przechowywane za pomocą środków elektronicznych w formie zapisów w pamięci ulotnej i/lub stałej, przetwarzane za pomocą Systemu Informatycznego;
11) **Postać tradycyjna danych** – dane w formie papierowej, przetwarzane za pomocą tradycyjnych metod składowania (np. w segregatorach, teczkach, na pułkach);
12) **Podmiot Przetwarzający (Przetwarzający, Procesor)** – osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
13) **Przetwarzanie** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
14) **Profilowanie** – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
15) **Rozliczalność** – rozumie się jako właściwość zapewniająca, że działania podmiotu (osoby) mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (tej osobie);
16) **Naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do
   przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych

przesyłanych,
przechowywanych lub w inny sposób przetwarzanych;

17) **System informatyczny Administratora Danych, System Asystent EFS (system informatyczny)** –rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych, telefony komórkowe, systemy e-mail lub inne, gdzie przetwarzane są dane osobowe w formie elektronicznej;
18) **Użytkownik** – osoba upoważniona do dostępu i przetwarzania danych osobowych, której nadano
identyfikator Użytkownika i przyznano hasło do systemów informatycznych;
19) **Zbiór danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych
według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
20) **Polityka Bezpieczeństwa Danych Osobowych (Polityka, Polityka Bezpieczeństwa**) – niniejszy dokument określający nadrzędne zasady ochrony danych osobowych u Administratora wraz z załącznikami i dokumentami stworzonymi na ich podstawie.
21) **Osoba związana z Administratorem** – podmiot danych osobowych, dla którego Project Hub Sp. z o.o. z/s w Poznaniu jest Administratorem danych osobowych w rozumieniu RODO. Może nim być w szczególności pracownik, współpracownik, kontrahent, pracownicy kontrahenta, klient, darczyńca, osoby kontaktujące się przez kanały elektroniczne lub w sposób tradycyjny.

§2 Cele i zasady funkcjonowania Polityki Bezpieczeństwa

1. Niniejsza Polityka zapewnia:

1) Spójność z wyznaczonymi zadaniami oraz pełną integrację z podstawowymi procedurami
zdefiniowanymi u Administratora;
2) Skuteczne działania w odniesieniu do zagrożeń poufności, integralności i dostępności danych
osobowych, realizację zadań Administratora w taki sposób, aby podnieść jakość i wiarygodność Project Hub Sp. z o.o. z/s w Poznaniu oraz aby zapewnić rozliczalność przetwarzania danych osobowych i bezpieczeństwo ich praw;
3) Ochronę danych osobowych tworzonych, przetwarzanych, przechowywanych i przesyłanych
nie tylko za pomocą systemów informatycznych, ale również i w sposób tradycyjny;
4) Zgodność z materialnym zakresem stosowania RODO, co oznacza, że ma zastosowanie do
przetwarzania danych osobowych w sposób całkowicie lub częściowo

zautomatyzowanych oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących częśćzbioru danych lub mających stanowić część zbioru danych.

2. Celem Polityki Bezpieczeństwa Danych Osobowych oraz jej załączników i dokumentów wewnętrznych stosowanych przez Administratora jest wskazanie działań, jakie należy podejmować oraz ustanowienie zasad, jakie należy stosować, aby prawidłowo były realizowane obowiązki Administratora Danych Osobowych w zakresie zabezpieczenia udostępnionych oraz powierzonych mu danych osobowych.
3. Realizując niniejszą Politykę bezpieczeństwa, Administrator przyjmuje następujące zasady w zakresie:
   1) Poufności – dane nie są udostępniane lub ujawniane podmiotom bądź osobom nieupoważnionym;
   2) Integralności – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany;
   3) Dostępności – istnieje możliwość wykorzystania danych na żądanie, w założonym czasie, przez autoryzowany podmiot;
   4) Rozliczalności – możliwość jednoznacznego przypisania działań dotyczących danych poszczególnym osobom;
   5) Autentyczności – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
   6) Niezawodności – zamierzone zachowania i skutki są spójne;
4. Administrator przetwarza dane:
   1) zgodnie z prawem, rzetelnie i w sposób przejrzysty (zasada zgodności z prawem, rzetelności, przejrzystości),
   2) w sprecyzowanych, wyraźnie i prawnie uzasadnionych celach (zasada ograniczenia celu),
   3) tylko w takim zakresie, jaki jest niezbędny dla osiągnięcia celu ich zbierania (zasada minimalizacji danych),
   4) w formie aktualnej, umożliwiającej identyfikację osoby, przez czas niezbędny dla realizacji celu ich zbierania, a w razie potrzeby są uaktualniane, aby dane nieprawidłowe zostały usunięte lub sprostowane (zasada prawidłowości danych),
   5) w formie umożliwiającej identyfikację osoby, której dane dotyczą przez ograniczony okres, nie dłuższy, niż jest to niezbędne do celów, w których dane są przetwarzane (zasada ograniczenia przechowywania),

6) w sposób zapewniający odpowiednie bezpieczeństwo przed ich nieuprawnioną zmianą czy zniszczeniem (zasada integralności i poufności),

7) w sposób umożliwiający wykazanie przestrzegania tych zasad (zasada rozliczalności).

5. Polityka Bezpieczeństwa Danych Osobowych ma na celu zredukowanie, a ostatecznie wyeliminowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone;

2) naruszeń przepisów prawa oraz innych regulacji;

3) utraty lub obniżenia reputacji podmiotów, których dane dotyczą;

4) strat finansowych Administratora ponoszonych w wyniku nałożonych kar;

5)zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemu, a w szczególności niedoprowadzenia u osób związanych z organizacją do uszczerbku fizycznego lub

szkód majątkowych lub niemajątkowych, jeżeli nieuprawnione przetwarzanie mogłoby skutkować:

dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych lub wszelką inną znaczną szkodą gospodarczą lub społeczną, jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi.

§ 3 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

1. Administrator Danych Osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków, w tym zwłaszcza:

a) wprowadza właściwe procedury i zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych oraz monitoruje ich przestrzeganie,

b) informuje pracowników na temat obowiązujących przepisów, zasad i wewnętrznych procedur

ochrony danych osobowych, w tym zapoznaje ich z zapisami niniejszej Polityki

c) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur

bezpiecznego przetwarzania danych osobowych,

d) sprawdza aktualność polityk, zasad i procedur ochrony danych osobowych, a w szczególności

aktualizuje na bieżąco Rejestr Czynności Przetwarzania, Rejestr Kategorii Czynności Przetwarzania, Ewidencję zbiorów danych osobowych oraz Rejestr naruszeń.

e) jeżeli uzna za zasadne lub wymagają tego przepisy prawa, ponownie przeprowadza określenie i szacowanie ryzyka.

2. Administrator Danych Osobowych realizuje również zadania w zakresie zarządzania i bieżącego nadzoru nad Systemem Informatycznym, w tym zwłaszcza:
   a) zarządza Systemem Informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji Administratora,
   b) przeciwdziała dostępowi osób niepowołanych do Systemu Informatycznego, w którym przetwarzane są dane osobowe,
   c) zarządza uprawnieniami i jeżeli wynika taka konieczność, udziela dostęp poszczególnym Użytkownikom (poprzez identyfikatory, hasła) do Systemu Informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta Użytkowników,
   d) podejmuje działania zapewniające integralność danych w sytuacji stwierdzenia naruszenia zabezpieczeń Systemu Informatycznego;
   e) sprawuje nadzór nad wykonywaniem napraw, konserwacją, uaktualnianiem oraz likwidacją urządzeń komputerowych i systemów informatycznych, na których zapisane są dane osobowe i nad wykonywaniem kopii zapasowych.
3. Administrator prowadzi i na bieżąco aktualizuje wykaz osób upoważnionych do gromadzenia i przetwarzania danych osobowych, który powinien zawierać następujące dane:
   1) nazwisko i imię osoby upoważnionej,
   2) identyfikator osoby upoważnionej w systemie informatycznym (jeśli dotyczy),
   3) stanowisko,
   4) wskazanie zbiorów danych osobowych, do którego osoba upoważniona ma prawo dostępu,
   5) zakres uprawnień danej osoby w zakresie przetwarzania danych osobowych,
   6) datę przyznania uprawnień,
   7) termin wygaśnięcia uprawnień,
   8) zobowiązanie do zachowanie poufności,
   9) oświadczenie o zapoznaniu się z niniejszą Polityką i zobowiązanie do jej przestrzegania.

§4 Rejestr czynności przetwarzania

1. Administrator prowadzi Rejestr Czynności Przetwarzania danych osobowych. W rejestrze tym zamieszcza się w szczególności wszystkie następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe Administratora,
b) cele przetwarzania danych osobowych,
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców
w państwach trzecich lub w organizacjach międzynarodowych (o ile dotyczy)
e) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
f) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa
danych.

2. Rejestr Czynności Przetwarzania obejmuje zarówno zbiory danych przetwarzanych w wersji
elektronicznej jak i zbiory danych przechowywane w wersji papierowej.

§5 Powierzenie danych podmiotom zewnętrznym

1. Powierzenie danych przetwarzanych przez Administratora może nastąpić w drodze pisemnej umowy powierzenia danych osobowych, w której podmiot przyjmujący dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych oraz zasad wynikających z RODO. Umowa powinna zawierać informacje wynikające z art. 28 RODO.
2. Administrator zawiera umowy powierzenia bądź dba o wprowadzenie odpowiednich klauzul odnoszących się do zapewnienia bezpieczeństwa danych osobowych w ramach powierzenia, z umowami określającymi współpracę ze wszystkimi podmiotami zewnętrznymi, którym zleca przetwarzanie danych.

§6 Pomieszczenia tworzące obszar, w którym przetwarzane są dane osobowe

1. Pomieszczeniami tworzącymi obszar, w którym znajdują się przetwarzane dane osobowe są
pomieszczenia, w których znajdują się zbiory danych w formie kartotek, rejestrów, segregatorów,
czyli danych papierowych oraz systemy informatyczne, w których są przetwarzane dane osobowe.
2. Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru, o którym mowa w ust. 1, osób nieuprawnionych do dostępu do danych osobowych, powinno być zorganizowane w sposób uniemożliwiający zapoznanie się tym osobom z przetwarzanymi przez Administratora danymi osobowymi.

3. Meble oraz inne schowki, w których przechowywane są dane osobowe powinny być zamykane
   i chronione przed dostępem do nich osób nieupoważnionych do przetwarzania danych osobowych.
4. W przypadku zamykanych na klucz szaf, schowków i pomieszczeń, w których przechowywane są
   dane osobowe, Administrator prowadzi rejestr kluczy, w tym osób posiadających upoważnienia do systemów informatycznych, a dokumenty z danymi udostępniane są wyłącznie osobom upoważnionym przez Administratora, w tym podmiotom przetwarzającym.

§7 Osoby upoważnione przez Administratora

1. Każda osoba zatrudniona u Administratora lub z nim współpracująca, bądź podmioty, których Administrator upoważnił do przetwarzania danych osobowych, są zobowiązane do przestrzegania następujących zasad ogólnych dotyczących bezpieczeństwa ochrony danych osobowych tj.:
   1) dbanie o poufność, dostępność i zachowanie integralności przetwarzanych danych osobowych,
   2) przetwarzanie danych osobowych wyłącznie w czasie i w zakresie ustalonym indywidualnie
   przez Administratora w upoważnieniu lub w umowie powierzenia oraz wyłącznie w celu wykonywania nałożonych na nią obowiązków, w tym praw wynikających z przepisów prawnych,
   3) zachowanie w poufności danych osobowych oraz przestrzeganie procedur ich bezpiecznego
   przetwarzania. Przestrzeganie zasady poufności danych osobowych obowiązuje przez cały
   okres zatrudnienia lub wykonywania zlecenia bądź umowy powierzenia na rzecz Administratora, a także po ustaniu współpracy zgodnie z właściwymi regulacjami ustawowymi lub umownymi,
   4) dopuszczenie do przetwarzania danych osoby/podmioty znające przepisy w zakresie ochrony danych oraz postanowienia niniejszej Polityki służące do przetwarzania danych osobowych,
   5) stosowanie określonych przez Administratora procedur i wytycznych mających na celu przetwarzanie danych osobowych zgodnie z obowiązującym prawem oraz realizacje praw podmiotów danych,
   6) niedopuszczenie osób nieuprawnionych do elektronicznych/papierowych nośników danych
   w których znajdują się dane osobowe podmiotów, z którymi współpracuje

Administrator, a w razie stwierdzenia takiego nieuprawnionego dostępu, niezwłoczne informowanie Administratora,

7) korzystanie z Systemu Informatycznego w sposób zgodny ze wskazówkami zawartymi

w instrukcjach obsługi urządzeń wchodzących w skład Systemu Informatycznego, oprogramowania i nośników oraz stosowanie higieny hasła,

8) zabezpieczenie danych na wszystkich rodzajach nośników, z których osoba/podmiot korzysta, przed ich udostępnianiem osobom nieupoważnionym (np. przy pomocy szyfrowania, hasła).

§8 Zabezpieczenia zbiorów danych w wersji papierowej oraz innych nośników danych

1. Gwarancją zapewnienia bezpieczeństwa Systemu Informatycznego oraz przetwarzanych i przechowywanych danych osobowych jest zapewnienie bezpieczeństwa fizycznego, organizacyjnego i technicznego.
2. Zabezpieczenia danych osobowych, w tym zabezpieczenia systemów informatycznych (fizyczne,
   organizacyjne, techniczne) stanowią prawnie chronioną tajemnicę przedsiębiorstwa, której
   pracownicy bądź osoby współpracujące są zobowiązani zachować w tajemnicy w trakcie trwania
   stosunku prawnego oraz po jego zakończeniu.
3. Ochronę gromadzonych zbiorów danych stanowią:
   a) antywłamaniowe drzwi na podwójny klucz do biura Administratora,
   b) zamykane szafy z danymi osobowymi,
   c) przyznawanie upoważnień dostępu do przetwarzania danych, w tym w systemach informatycznych,
   d) zapoznanie upoważnionych osób z zasadami ochrony danych,
   e) ustawienie monitorów w sposób uniemożliwiający osobom nieupoważnionym dostępu do
      danych osobowych wyświetlanych na nich,
   f) przydzielanie haseł dostępu do systemu informatycznego i indywidualnych kont,
   g) systematyczna zmiana haseł dostępu do systemu informatycznego i indywidualnych kont,
   h) posiadanie kopii danych,
   i) współpraca z agencją ochrony (jeżeli dotyczy),
   j) zabezpieczenie systemu informatycznego programami antywirusowymi niedopuszczającymi
      do zainfekowania szkodliwym oprogramowaniem,

k) zakaz wynoszenia danych na niezaszyfrowanych pamięciach przenośnych poza obszar
przetwarzania, a dane zgrane na pamięci przenośne nie powinny być dłużej na nich przechowywane niż jest to konieczne,
l) szkolenia z ochrony danych pracowników,

4. Należy chronić dokumenty papierowe jak i nośniki magnetyczne i optyczne (płyty, pendrive itp.) zawierające dane osobowe przed ich fizycznym uszkodzeniem lub zniszczeniem, co uniemożliwiałoby odczytanie lub odzyskanie informacji w nich zawartych.
5. Dokumenty papierowe oraz nośniki magnetyczne i optyczne zawierające dane osobowe muszą być chronione przed zagrożeniami ze strony otoczenia, kradzieżą lub niewłaściwym używaniem (ogień, wyciek wody, kradzież itp.). Opuszczając stanowisko pracy należy sprawdzić, czy są one zamknięte w odpowiednich szafach oraz innych zabezpieczonych schowkach. Klucze do zamykanych szaf oraz schowków, gdzie przechowywane są dane, nie mogą być pozostawiane w drzwiach lub w innym miejscu ogólnie dostępnym dla osób nieupoważnionych.
6. Zabrania się przekazywania lub udostępniania dokumentów papierowych lub innych nośników zawierających dane osobowe osobom nieuprawnionym.
7. Zabrania się kopiowania jakichkolwiek danych osobowych zawartych na dokumentach papierowych lub innych nośnikach bez zgody Administratora lub osoby przez niego upoważnionej.
8. Usunięcie lub wyniesienie poza siedzibę podmiotu dokumentu papierowego lub innego nośnika zawierającego dane osobowe wymaga zgody Administratora lub upoważnionej przez niego osoby.
9. Utrata, kradzież lub uzyskanie dostępu przez osobę nieuprawnioną do dokumentów papierowych lub innych nośników zawierających dane osobowe powinna być niezwłocznie zgłoszona Administratorowi.
10. Każdy dokument papierowy zawierający dane osobowe który nie podlega archiwizacji, należy zniszczyć w sposób trwały, uniemożliwiający odczytanie danych osobowych. W przypadku innych nośników, zapisane dane, które nie podlegają archiwizacji należy usunąć w sposób uniemożliwiający ich odczytanie.

§ 9 Zgłaszanie i zawiadamianie o naruszeniu ochrony danych osobowych

1. Każde naruszenie ochrony danych osobowych powinno być niezwłocznie zgłaszane przez użytkowników Administratorowi. Szczegóły w zakresie postępowania w związku ze stwierdzonym naruszeniem ochrony danych osobowych przy korzystaniu z Systemu Informatycznych opisane zostały w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych stanowiącymi załącznik do Polityki Bezpieczeństwa Danych Osobowych.
2. Administrator danych osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte środki zaradcze. Dokumentacja odbywa się z wykorzystaniem zestawienia incydentów naruszenia ochrony danych osobowych.
3. W przypadku naruszenia ochrony danych osobowych, na administratorze danych osobowych ciąży obowiązek zgłoszenia tego faktu do organu nadzorczego zgodnie z postanowieniami art. 33 RODO oraz zawiadomienia osoby, której dane dotyczą, zgodnie z postanowieniami art. 34 RODO.

§ 10 Postawienia końcowe

1. Administrator prowadzi ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
2. Wszelkie załączniki do Polityki Bezpieczeństwa Danych Osobowych w tym Instrukcja Zarządzania Systemem Informatycznym stanowią jej integralną część.
3. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustaw
   szczególnych, RODO oraz umowy zawarte z podmiotami przetwarzającymi dane.