POLITYKA BEZPIECZEŃSTWA

przetwarzania danych osobowych w Specjalnym Ośrodku Szkolno – Wychowawczym im. Mieszka I w Chojnie

wg. 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)

SPIS TREŚCI:

I. DOKUMENTACJA DOTYCZĄCA SPOSOBU PRZETWARZANIA DANYCH

I. DOKUMENTACJA DOTYCZĄCA SPOSOBU PRZETWARZANIA DANYCH OSOBOWYCH

I.1. Definicje :

1) **„RODO"** ROZPORZĄDZENIE 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);

2) **„ustawa"** Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. poz. 1000 i 1699);

3) **„inspektor ochrony danych „** osoba , podmiot powołany przez administratora danych do realizacji zadań wynikających z RODO celem skutecznej ochrony danych osobowych ;

4) **„administrator systemu informatycznego"** osoba, podmiot nadzorujący i odpowiadający za poprawną pracę powierzonego mu sprzętu sieciowego oraz systemu operacyjnego, oprogramowania instalowanego w danej jednostce organizacyjnej;

5) **„dane osobowe"** oznaczają 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;

6) **„przetwarzanie"** oznacza 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;

7) **„incydent"** naruszenie ochrony danych osobowych w sposób zamierzony lub niezamierzony , które może powodować stratę oraz skutki negatywne dla bezpieczeństwa zasobów;

8) **„ograniczenie przetwarzania"** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

9) **„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;

10) **„pseudonimizacja"** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami

technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

11) **„zbiór danych"** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

12) **„administrator"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

13) **„podmiot przetwarzający"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

14) **„odbiorca"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

15) **„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;

16) **„zgoda" osoby** której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

17) **„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;

18) **„dane genetyczne"** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

19) **„dane biometryczne"** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz

umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

20) **„dane dotyczące zdrowia"** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

21) **„przedstawiciel"** oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;

22) **„przedsiębiorca"** oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;

23) **„organ nadzorczy"** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51;

24) **„identyfikator użytkownika"** ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

25) **„hasło"** ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy
w systemie informatycznym;

26) **„system informatyczny"** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

27) **„zgodność przetwarzania danych osobowych „** - przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:
    a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
    b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
    c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
    d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
    e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
    f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

28) **„warunki wyrażenia zgody"**

a) Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
b) Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.
c) Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
d) Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy

29) **„przetwarzanie szczególnych kategorii danych osobowych"**

Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Powyższe nie dotyczy wówczas gdy został spełniony jeden z warunków zawartych w art.9 ust.2 RODO

30) **„ośrodek"** Specjalny Ośrodek Szkolno – Wychowawczy im. Mieszka I w Chojnie

I.2. WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące zapewnienia bezpieczeństwa danych osobowych zawartych w Specjalnym Ośrodku Szkolno – Wychowawczym im. Mieszka I w Chojnie. Opisane reguły określają granice dopuszczalnego zachowania wszystkich, którzy przetwarzają dane osobowe w ośrodku.

Dokument zwraca uwagę na konsekwencje, jakie mogą wynikać z niewłaściwego przetwarzania danych osobowych oraz procedury postępowania dla zapobiegania i minimalizacji skutków zagrożeń.

Dokument polityka bezpieczeństwa przetwarzania danych osobowych zgodnie z RODO, określa sposób postępowania celem minimalizacji naruszenia bezpieczeństwa przy przetwarzaniu danych osobowych, a także sposób postępowania w sytuacji wystąpienia incydentu.

Potrzeba opracowania polityki bezpieczeństwa wynika z przepisów art. 24 RODO, który do obowiązków administratora zalicza wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się zgodnie z rozporządzeniem i aby móc to wykazać.

Zasady stosowanych środków powinny uwzględniać charakter, zakres i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki , o których mowa powyżej obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

I.3. PRZEPISY OGÓLNE

1. Celem polityki bezpieczeństwa jest wdrażanie odpowiednich metod, które spowodują właściwe postępowanie i zabezpieczenie zasobów związanych z przetwarzaniem danych osobowych.
2. Polityka bezpieczeństwa określa tryb i zasady postępowania w przypadku , gdy:
    1) ujawnione zostaną sytuacje wskazujące na wystąpienie incydentu z naruszeniem ochrony danych osobowych;
    2) zostały zanalizowane określone ryzyka naruszenia celem minimalizacji ryzyka.

3. Realizacja zapisów w „Polityce bezpieczeństwa" ma zapewnić właściwą i skuteczną reakcję, ocenę
   i dokumentowanie przypadków wystąpienia incydentów.
4. Zasady realizacji zadań ciążących na Inspektorze ochrony danych.
5. Administrator swoją decyzją wyznacza inspektora ochrony danych osobowych.

I.4. INSPEKTOR OCHRONY DANYCH OSOBOWYCH

1. Zadaniem inspektora ochrony danych jest działanie na rzecz zgodnego z przepisami o ochronie danych przetwarzania danych.
2. Administrator oraz podmiot przetwarzający ma obowiązek właściwego i bezzwłocznego włączania Inspektora we wszystkie sprawy dotyczące ochrony danych osobowych (art. 38 ust. 1 RODO). Administrator danych lub podmiot przetwarzający powinien umożliwić inspektorowi ochrony danych czynny udział we wszystkich sprawach dotyczących procesów przetwarzania danych osobowych oraz na bieżąco przekazywać mu wszystkie informacje związane z wykonywaniem jego zadań. Tym samym wiedza inspektora ma obejmować informacje o każdej sprawie dotyczącej przetwarzania i ochrony danych osobowych, w danej jednostce organizacyjnej.
3. Inspektor ochrony danych, w związku z pełnieniem swojej funkcji, realizuje swoje zadania rzetelnie a także charakteryzuje się wysokim poziomem etyki zawodowej oraz poprzez priorytetowe traktowanie swoich obowiązków.
4. Inspektor w zakresie swoich obowiązków podlega bezpośrednio administratorowi. Administrator wspiera Inspektora w wypełnianiu jego zadań.
5. Administrator zapewnienia udział Inspektora we wszystkich zagadnieniach związanych z ochroną danych osobowych.
6. Administrator nie powinien wydawać inspektorowi instrukcji co do wykonywania przez niego zadań.

I.5. ZADANIA INSPEKTORA OCHRONY DANYCH

1. Informowanie administratora, oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia (RODO) oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.

2. Monitorowanie przestrzegania przepisów krajowych, rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych
3. Podejmowanie działań zwiększające świadomość pracowników przetwarzających poprzez szkolenia personelu uczestniczącego w operacjach przetwarzania.
4. Prowadzenie okresowych przeglądów stanu zabezpieczenia danych osobowych, audytów i przedstawianie ich wyników administratorowi danych osobowych.
5. Realizacja zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania.
6. Współpraca z organem nadzorczym.
7. Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
8. W przypadku incydentu związanego z naruszeniem ochrony danych osobowych pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia (RODO).
9. Prowadzenie rejestru czynności na zbiorach.
10. Prowadzenie dokumentacji dla administratora danych osobowych.
11. Prowadzenie spraw związanych z incydentami, w przypadku ich wystąpienia.
12. Dokonywanie oceny i szacowania ryzyka celem zastosowania skutecznych metod organizacyjnych
    i technicznych dla właściwej ochrony danych osobowych u administratora danych osobowych, a w przypadku potrzeby oceny skutków naruszenia ochrony danych osobowych.
13. Przygotowywanie do podpisania przez administratora poleceń -upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób poleceń- upoważnionych.

I.6. ZADANIA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

1. Dokonywanie zmian uprawnień użytkowników.
2. Nadzór nad funkcjonowaniem systemu informatycznego.
3. Kontrola użytkowników w zakresie uprawnień ich dostępu.
4. Współpracuje z Inspektorem Danych Osobowych w przypadku naruszenia zabezpieczeń w systemie.
5. Dokonuje napraw sprzętu komputerowego oraz przeglądu.
6. Aktualizuje oprogramowania, w tym programy antywirusowe.

I.7. PRZETWARZANIE DANYCH OSOBOWYCH – ZASADY OGÓLNE

1. Wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne.
2. Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane.
3. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.

4. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących.
5. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem.
6. Konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.
7. Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum.
8. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami.
9. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu.
10. Należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe.
11. Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

I.8. ZASADY STOSOWANIA ŚRODKÓW TECHNICZNYCH I ORGAIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I DOSTĘPNOŚCI PRZETWARZANIA DANYCH

Poufność – właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom.

Integralność – właściwość zapewniająca, że informacje nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Dostępność - właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.

1. Przydzielany jest identyfikator użytkownika i stosowane jest hasło dostępu,
2. Każdy użytkownik ma obowiązek zablokowania stacji roboczej lub wylogowania się z systemu informatycznego służącego do przetwarzania danych osobowych w przypadku czasowego opuszczenia stanowiska pracy,
3. Każdorazowe zakończenie pracy w systemie służącym do przetwarzania danych osobowych poprzedzone jest zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych, takich jak dyskietki, płyty CD i inne, zawierających dane osobowe,
4. Obowiązuje zakaz wynoszenia poza pomieszczenia stanowiące obszar przetwarzania danych osobowych elektronicznych nośników informacji zawierających dane osobowe oraz kopie zapasowe bez wiedzy Inspektora.
5. W sytuacji przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez

fizyczne wymontowanie dysku lub skasowanie danych, jeśli jest to możliwe naprawa powinna zostać przeprowadzona w obecności Administratora Bezpieczeństwa Informacji.
6. Ekrany monitorów usytuowane są w sposób uniemożliwiający wgląd, obserwację przetwarzania danych przez osoby postronne.

I.9. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ PRACOWNIKÓW

1. Zgodnie z art. 29 RODO - podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.
2. Wzór polecenia upoważnienia – polecenia stanowi załącznik nr 2 do polityki bezpieczeństwa.
3. Prowadzony jest rejestr osób upoważnionych do przetwarzania danych osobowych.

I.10. PODMIOT PRZETWARZAJĄCY - UMOWA POWIERZENIA

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
3. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
4. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
5. Umowa powierzenia jest podpisana na piśmie lub w formie elektronicznej.
6. Wzór umowy powierzenia stanowi załącznik nr 5.

I.11. REJESTROWANIE CZYNNOŚCI - ZASADY

1.Zgodnie z Rozporządzeniem ogólnym UE w sprawie ochrony danych osobowych, administrator danych prowadzi rejestr czynności przetwarzana danych osobowych. Jest to dokument, który ma pokazywać w szczególności w jakich procesach w organizacji są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jak są zabezpieczane. Dokument ten będzie musiał zostać udostępniony na każde wezwanie GIODO.
2.Celem prowadzenia ww. rejestru jest możliwości pełnienia nadzoru i monitorowania procesów przetwarzania danych osobowych przez organ nadzorczy.
3. Rejestr czynności przetwarzania prowadzony przez ADO wg.RODO jest prowadzony wówczas gdy przetwarzanie :

- może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą;
- nie ma charakteru sporadycznego;

- obejmuje szczególne kategorie danych osobowych ;
- obejmuje dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o których mowa w art. 10 RODO.

4. Rejestr może być prowadzony w formie pisemnej bądź elektronicznej.
5. Administrator lub podmiot przetwarzający oraz przedstawiciel administratora lub podmiotu przetwarzającego (jeżeli istnieje) mają obowiązek udostępnić rejestr na każde żądanie organu nadzorczego. Organ nadzorczy dokonuje kontroli tych rejestrów w celu monitorowania operacji przetwarzania.
6. Rejestr czynności przetwarzania prowadzony przez administratora danych zawiera:

- nazwę i dane kontaktowe administratora danych;
- nazwy współadministratorów – jeżeli istnieją;
- nazwę przedstawiciela;
- dane kontaktowe inspektora jeżeli został powołany,
- kategorie osób, których dane dotyczą /nazwa zbioru/;
- kategorie danych osobowych;
- kategorie odbiorców, którym dane zostały lub zostaną udostępnione;
- cel przetwarzania danych;
- informację o przekazywaniu danych do państwa trzeciego wraz z dokumentacją opisującą zastosowane zabezpieczenia w tym procesie;
- planowany termin usunięcia danych osobowych;
- ogólny opis zastosowanych zabezpieczeń technicznych i organizacyjnych.

7. Rejestr czynności przetwarzania danych stanowi załącznik nr 1 do polityki bezpieczeństwa.

I.12. INCYDENTY

1. Rozporządzenie 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 nakłada na administratora danych obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych;.
2. Zasady zgłaszania naruszenia ochrony danych organowi nadzorczemu określone są w artykule 33 RODO.
3. Administrator danych osobowych ma obowiązek zgłoszenia organowi nadzorczemu przypadek naruszenia ochrony danych osobowych w ciągu 72 godzin. Jeżeli zgłoszenie przekazane zostanie po 72 godz. należy wówczas dołączyć wyjaśnienie przyczyn opóźnienia.
4. Zwolnienie z obowiązku zgłoszenia naruszenia, organowi nadzorczemu możliwe jest, jeżeli jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
5. Jeżeli naruszenie dotyczy podmiotu przetwarzającego, to podmiot przetwarzający bez zbędnej zwłoki zgłasza je administratorowi danych;

- jeżeli informacji nie możemy udzielić w tym samym czasie możemy je przekazywać organowi nadzorczemu sukcesywnie bez zbędnej zwłoki;
- administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania artykułu 33 RODO;
- administrator prowadzi rejestr incydentów – wzór rejestru stanowi załącznik nr 6 do Polityki.

I.13. ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH.

1. Jeżeli 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.
2. Zawiadomienie, jasnym i prostym językiem powinno opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej niżej wymienione informacje:
   - imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   - opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   - opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

I.14. Zawiadomienie nie jest wymagane w następujących przypadkach:

1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.
2. Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt. 1.
3. Wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, wymienionych wyżej.
5. Wzór zawiadomienia stanowi załącznik nr 7 do polityki bezpieczeństwa.

I.15. OBOWIĄZEK INFORMACYJNY –ZASADY

1. Motyw 60 preambuły RODO wskazuje nam, że osoba, której dane dotyczą, musi być poinformowana o **prowadzeniu operacji przetwarzania i o jego celach**. Poza tym administrator powinien podać wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.
2. Dodatkowo należy poinformować o fakcie **profilowania** oraz o konsekwencjach takiego profilowania. W przypadku zbierania danych od osoby, której dane dotyczą, należy wskazać, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania.

I.15.1 O CZYM POWINNISMY POINFORMOWAĆ ZBIERAJAC DANE OD OSOBY, KTÓREJ DANE DOTYCZĄ?

W przypadku, gdy zbieramy dane osobowe, od osoby której dane dotyczą zgodnie z art. 13 ust. 1 i 2 RODO powinniśmy poinformować ją o:
a) swojej tożsamości i danych kontaktowych oraz tożsamość i danych kontaktowych swojego przedstawiciela, jeżeli istnieje;
b) danych kontaktowych inspektora ochrony danych (jeżeli go powołaliśmy);
c) celach przetwarzania, do których mają posłużyć dane osobowe;

d) podstawie prawnej przetwarzania;
f) prawnie uzasadnionym interesie realizowanym przez administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu ADO ;
g) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
h) transferze danych do państwa trzeciego, w tym o:

- zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej ,
- stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony ,
- lub wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego ,

i) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
j) prawie do:

- żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą,
- ich sprostowania, usunięcia lub ograniczenia przetwarzania lub
- wniesienia sprzeciwu wobec przetwarzania, a także
- przenoszenia danych;

k) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych zwykłych lub szczególnej kategorii ;
l) prawie wniesienia skargi do organu nadzorczego;
m) informacji, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
n) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

I.15.2 O CZYM POWINNIŚMY POINFORMOWAĆ ZBIERAJĄC DANE Z INNEGO ŹRÓDŁA NIŻ OSOBA, KTÓREJ DANE DOTYCZĄ?

W przypadku, gdy zbieramy dane osobowe, od innego źródła niż od osoby której dane dotyczą zgodnie z art. 14 ust. 1 i 2 RODO powinniśmy poinformować ją o:
a) informacjach z punktów a-l oraz n wskazanych powyżej;
b) kategoriach odnośnych danych osobowych
c) źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

I.15.3. FORMA OBOWIĄZKU INFORMACYJNEGO

1. Powyższe informacje administrator danych powinien przekazać w **formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej** oraz jasnym i prostym językiem w szczególności gdy informacje są kierowane do dziecka (art. 12 ust. 1 RODO).
2. Klauzulę informacyjną można opatrzyć też **standardowymi znakami graficznymi**, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania (Art. 12 ust. 7 RODO),
3. Obowiązek informacyjny możemy spełnić **na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie**. Jednak jeżeli w treści obowiązku informacyjnego zastosowano znaki, a

są one przedstawione elektronicznie, muszą nadawać się do odczytu maszynowego. Dodatkowo spełnienie obowiązku informacyjnego w stosunku do osób musi być wolne od opłat.

I.16. PRAWO DO KONTROLI.

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dotyczące jej dane osobowe. Jeżeli dane są przez dany podmiot przetwarzane, to może wnioskować o udzielenie następujących informacji:
1) cele przetwarzania;
2) kategorie danych osobowych;
3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) informacje o prawie wniesienia skargi do organu nadzorczego;
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
9) jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

I.16.1 OBOWIĄZEK UŁATWIANIA KONTROLI

Administrator ma obowiązek ułatwiania osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22:

1. Prawo dostępu do swoich danych ,
2. Prawo do sprostowania,
3. Prawo do usunięcia,
4. Prawo do ograniczenia,
5. Prawo do przenoszenia,
6. Prawo do sprzeciwu,
7. Prawo do informacji o profilowaniu.

Również w przypadkach przetwarzania niewymagającego identyfikacji, administrator nie może odmawiać podjęcia działań na żądanie osoby chcącej zrealizować prawa przysługujące jej na mocy art. 15–22, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.

I.16.2. OBOWIĄZEK INFORMOWANIA –TERMINY

1. **bez zbędnej zwłoki** – a w każdym razie w terminie miesiąca od otrzymania żądania- zasadniczo,

2. **trzy miesiące** – w razie potrzeby ww. termin jednego miesiąca można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań,
3. w terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia,
4. jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

I.16.3. OBOWIĄZEK UZASADNIENIA ODRZUCENIA ŻĄDANIA - POUCZENIE O PRAWIE SKARGI

Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o:
1) powodach niepodjęcia działań; oraz
2) możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

I.16.4. WOLNOŚĆ OD OPŁAT

Prawo do kontroli jest wolne od opłat jednakże:
jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:
1. pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
2). odmówić podjęcia działań w związku z żądaniem.
Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

I.16.5. OBOWIĄZKI OSOBY, KTÓREJ DANE DOTYCZĄ, WZGLĘDEM ADMINISTRATORA

1. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.
2. To, że wątpliwości muszą być uzasadnione, oznacza że administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. Administrator nie powinien zatrzymywać danych osobowych wyłącznie w celu reagowania na ewentualne żądania.
3. Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, może zażądać, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie.

I.17. ANALIZA I SZACOWANIE RYZYKA

Zgodnie z art.24 RODO na administratora oraz podmiot przetwarzający nałożony został obowiązek zastosowania zabezpieczeń danych osobowych zgodnie z oceną zagrożeń.

I.17.1. OBOWIĄZKI ADMINISTRATORA

1. 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 niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.
3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

I.17.2 UWZGLĘDNIENIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH.

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.
2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.
3. Każda organizacja przetwarzająca dane narażona jest na wpływ czynników wewnętrznych oraz zewnętrznych, które mogą spowodować naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem:
   - **zniszczenia,**
   - **utracenia,**
   - **zmodyfikowania,**
   - **nieuprawnionego ujawnienia,**
   - **nieuprawnionego dostępu**

4.Ocenę ryzyka w zakresie bezpieczeństwa przetwarzania danych osobowych przeprowadzamy biorąc pod uwagę potencjalnie negatywne skutki (straty) zarówno dla administratora jak i dla osób , których dane dotyczą.
5. Został opracowana analiza ryzyka ogólnego i ocena skutków dla Przetwarzania Danych.- załącznik nr 8 do polityki bezpieczeństwa.
UWAGA! Gdyby istniało wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, wówczas należy dodatkowo przeprowadzić ocenę skutków dla ochrony danych osobowych.

I.17.3 OGÓLNE WYMOGI BEZPIECZEŃSTWA

Przetwarzanie danych osobowych w ...Specjalnym Ośrodku Szkolno – Wychowawczym w Chojnie odbywa się w postaci:

- elektronicznej (np.: pliki na dysku komputera, w pamięci operacyjnej komputera),
- papierowej (wydruki).

Aby zapewnić bezpieczeństwo przetwarzania danych osobowych należy stosować:

- środki ochrony fizycznej stanowiska komputerowego oraz wydruków przed nieuprawnionym dostępem,
- środki ochrony technicznej stanowiska komputerowego (np.: hasła dostępu do stacji roboczej, program antywirusowy).

I.17.4 AKTYWA

1.Przetwarzanie danych osobowych odbywa się w Specjalnym Ośrodku Szkolno – Wychowawczym w Chojnie.
2. Dane osobowe przetwarzane są przez osoby uprawnione, posiadające upoważnienie wydane przez administratora danych osobowych.
3. Osoby upoważnione do przetwarzania danych osobowych odbywają obowiązkowe szkolenie z zakresu procedur i obowiązków związanych z prawidłowym przetwarzaniem danych osobowych. Po odbyciu szkolenia osoby przeszkolone składają pisemne oświadczenie o zapoznaniu z przepisami oraz o zachowaniu tajemnicy.
4. Prowadzona jest ewidencja wydanych upoważnień do przetwarzania danych osobowych oraz rejestr osób, które podpisały oświadczenie o zapoznaniu z przepisami- załącznik nr 3 do polityki bezpieczeństwa.
5. Prowadzony jest wykaz pomieszczeń stanowiących obszar przetwarzania danych osobowych – załącznik nr 4 do polityki bezpieczeństwa

I.17.5 EWENTUALNE KOSZTY ZWIAZANE Z UTRATĄ AKTYWÓW

1.Koszty związane z odtworzeniem aktywów.
2. Koszty utraty zaufania do administratora danych osobowych.
3. Koszty związane z utratą:
   - poufności,
   - integralności,
   - dostępności danych,
4. Możliwość nałożenia kary przez organ nadzorczy.
5. Koszty związane z możliwością nakazania przez organ nadzorczy całkowitego zaprzestania lub czasowego zaprzestania przetwarzania danych osobowych , np. w sytuacji niezastosowania przez administratora odpowiednich środków bezpieczeństwa.

I.17.6 ZAGROŻENIA DLA SYSTEMU INFORMATYCZNEGO

Podstawowe zagrożenia dla systemu informatycznego, przeznaczonego do przetwarzania danych osobowych:

I. utrata poufności (pozyskanie danych przez osoby nieupoważnione):

   - ✓ nieuprawniony dostęp do pomieszczenia gdzie znajdują się dane osobowe(wydruki)
   - ✓ nieuprawniony dostęp do stacji roboczej (komputera) gdzie znajdują się dane osobowe (np. poprzez ujawnienie hasła dostępu),
   - ✓ nieuprawnione skopiowanie danych osobowych na inny nośnik,
   - ✓ zgubienie nośnika zawierającego dane osobowe,
   - ✓ niedostateczne zniszczenie wydruku zawierającego dane osobowe,
   - ✓ klęska żywiołowa powodująca utratę poufności danych.

II. utrata integralności (zmiany w systemie informatycznym przeprowadzone przez osoby nieupoważnione):

- ✓ nielegalny dostęp do dokumentów zawierających dane osobowe (w formie papierowej i elektronicznej),
- ✓ błędy ludzkie,
- ✓ działania wirusów (brak programów antywirusowych i firewalli),
- ✓ awarie oprogramowania komputerów,

III. utrata rozliczalności (brak możliwości przypisania danemu podmiotowi konkretnych działań):

- ✓ brak mechanizmu uniemożliwiającego usunięcie logów o pracy danej osoby na komputerze,
- ✓ brak kontroli nad kopiowaniem dokumentów z komputera na nośniki zewnętrzne.

I.17.7 ANALIZA ZAGROŻEŃ I RYZYKA

1. Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.), określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie go zlikwidować.
2. Zagrożenia i ryzyka w zakresie ochrony danych osobowych:
   - Niedostateczne kwalifikacje Inspektora (w tym brak podnoszenia kwalifikacji),
   - Brak procedur ochrony danych osobowych,
   - Niezgodne z wymogami prawnymi, nieaktualne, nieadekwatne do zagrożeń procedury ochrony danych osobowych,
   - Brak aktualnego wykazu zbiorów będących w zasobach jednostki,
   - Brak lub wady upoważnień do przetwarzania danych osobowych,
   - Udzielanie upoważnienia do przetwarzania danych osobowych osobom postępującym nieetycznie,
   - Brak lub wady ewidencji wydanych upoważnień,
   - Brak lub wady szkoleń z zakresu ochrony danych osobowych,
   - Wady nadzoru nad przetwarzaniem i ochroną danych osobowych,
   - Brak lub wady identyfikacji i analizy ryzyka w zakresie przetwarzania i ochrony danych osobowych,
     Brak reakcji lub nieprawidłowa reakcja na zagrożenie bezpieczeństwa danych osobowych lub systemów i sieci teleinformatycznych.

I.17.8. POJĘCIE I CYKLE RYZYKA

1. Ryzyko jest mierzone wpływem (skutkami) i prawdopodobieństwem wystąpienia". Rozporządzenie w Artykule 32 definiuje cele w zakresie bezpieczeństwa przetwarzania i są to:
   - pseudonimizacja i szyfrowanie danych osobowych,
   - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
   - regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. W związku z powyższym ryzyko w przetwarzaniu danych jest związane z potencjalną sytuacją, w której określone zagrożenie wykorzysta podatność (np. niezabezpieczony hasłem sprzęt komputerowy), powodując w ten sposób szkodę dla jednostki organizacyjnej (np. kradzież lub upublicznienie informacji).

I.17.9 IDENTYFIKACJA RYZYKA (ZAGROŻEŃ I PODATNOŚCI)

Zgodnie z zapisem 75 punktu preambuły Rozporządzenia, wyszczególnione zostały zagrożenia związane z przetwarzaniem danych z wyszczególnieniem prowadzących do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:

- jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji 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,
- jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa,
- jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych,
- lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci,
- jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

II. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

II.1. POSTANOWIENIA OGÓLNE

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Specjalnym Ośrodku Szkolno – Wychowawczym w Chojnie określa:

1) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Specjalnym Ośrodku Szkolno – Wychowawczym w Chojnie, zwana dalej „Instrukcją" określa zasady , tryb postępowania i zalecenia Administratora Danych Osobowych , które należy stosować w trakcie przetwarzania danych osobowych w systemach informatycznych,
2) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,
3) sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
4) zasady i procedury rozpoczynania i kończenia pracy,
5) zasady i częstotliwość tworzenia kopii bezpieczeństwa.
6) zasady i częstotliwość kontroli obecności wirusów komputerowych oraz metodę ich usuwania,
7) zasady i czas przechowywania nośników informacji, w tym kopii informatycznych,
8) zasady dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
9) zasady postępowania w zakresie komunikacji w sieci komputerowej,

10) instrukcja opracowana została zgodnie z wymogami § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych w systemach informatycznych.

II.2. DEFINICJE ZAWARTE W INSTRUKCJI

Ilekroć w instrukcji jest mowa o:

1) **„identyfikator użytkownika"** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

2) **„hasło"** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

3) **„sieć telekomunikacyjna"** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)

4) **„sieć publiczna"** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;

5) **„teletransmisja"** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

6) **„rozliczalność"** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

7) **„integralność danych"** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

8) **„raport"** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

9) **„poufność danych"** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
10) **„uwierzytelnianie"** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

11) **„Administrator Systemu Informatycznego (ASI), zwanego też Administratorem Systemu"** - rozumie się przez to osobę zatrudnioną przez dyrektora Ośrodka upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;

12) **„użytkownik systemu informatycznego"** - rozumie się przez to upoważnioną przez dyrektora Ośrodka , pracownika do przetwarzania danych osobowych w systemie informatycznym , który odbył stosowne szkolenie w zakresie ochrony danych.

II.3. ZASADY DOSTĘPU UŻYTKOWNIKU DO SYSTEMU

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem" może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez Administratora Systemu na wniosek kierownika komórki organizacyjnej i po akceptacji Inspektora.
2. Rejestracja, o której mowa w ust. l, polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

II.4. IDENTYFIKATOR

1. Identyfikator składa się z minimum sześciu znaków.
2. W identyfikatorze pomija się polskie znaki diakrytyczne.
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu po uzgodnieniu z Inspektorem nadaje inny identyfikator.

II.5. HASŁA

1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.
3. Zmiana hasła następuje co miesiąc z zastrzeżeniem pkt II. 6.
4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

II.6. WYREJESTROWANIE UŻYTKOWNIKA

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek kierownika komórki organizacyjnej.
2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
3. Wyrejestrowanie następuje poprzez:
    - zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
    - usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:
    - nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
    - zawieszenie w pełnieniu obowiązków służbowych,
    - zwolnienie z pełnienia obowiązków służbowych.
4. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

II.7. ROZPOCZĘCIE PRACY W SYSTEMIE

Rozpoczęcie pracy w systemie odbywa się poprzez:
1) przygotowanie stanowiska pracy,
2) włączenie stacji roboczej,
3) wprowadzenie swojego identyfikatora i hasła.

II.8. ZAKOŃCZENIE PRACY W SYSTEMIE

Zakończenie pracy w systemie odbywa się poprzez:
1) zamknięcie aplikacji,
2) odłączenie się od zasobów systemowych,
3) zamknięcie systemu operacyjnego,
4) wyłączenie stacji roboczej.

II.9. ZASADY PRACY W SYSTEMIE

Zabrania się użytkownikom pracującym w systemie:
1) udostępniania stacji roboczej osobom niezarejestrowanym z zastrzeżeniem pkt 2,
2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Systemu Informatycznego,
3) używania nielicencjonowanego oprogramowania.

II.10. NARUSZENIE BEZPIECZEŃSTWA SYSTEMU

1. Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do Inspektora , a w szczególności:
a) naruszenia bezpieczeństwa systemu informatycznego,
b) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).
2. Inspektorowi Ochrony Danych zgłasza się w szczególności przypadki:
a) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
b) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
c) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),
d) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Administratora Danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
e) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,
f) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
g) przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
h) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.
3. Obowiązek dokonania zgłoszenia, o którym mowa w ust 1, spoczywa na każdym użytkowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.
4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem Administratora Systemu jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.
5. Użytkownik sieci i Administrator Systemu w porozumieniu z Inspektorem ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.
6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

II.11. KOPIA ZAPASOWA I PROGRAMY ANTYWIRUSOWE

1. Kopie awaryjne tworzy się z następującą częstotliwością:
a) kopie systemu finansowo - księgowego – dwa razy w miesiącu,
b) kopie pozostałe - nie rzadziej niż raz na kwartał.
2. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.
3. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.
4. Administrator Systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.

5. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia Administratora Systemu do ich zniszczenia.
6. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.
7. Oprogramowanie, o którym mowa w ust. 6, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
8. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, Administrator Systemu nie rzadziej niż raz na dwa miesiące przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
9. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

II.12. ZASILANIE AWARYJNE

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne (UPS).

II.13. NAPRAWA, SERWIS URZĄDZEŃ

1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, do likwidacji dopiero po uprzednim uzyskaniu zgody Inspektora.

2. Urządzenia, o których mowa w ust. I przed ich przekazaniem pozbawia się zapisu danych osobowych poprzez wymontowanie dysku twardego z zastrzeżeniem ust. 3.

3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemu.

4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.

II.14. PRZEGLAD, KONSERWACJE

1. Przeglądu i konserwacji systemu dokonuje Administrator Systemu doraźnie.

2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemu dokonuje nie rzadziej niż raz na dwa tygodnie.

3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu nie rzadziej niż raz na dwa tygodnie.

II.15. BEZPIECZEŃSTWO KOMUNIKACJI

1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe Administrator Systemu zapewnia przy użyciu narzędzi w obrębie systemu.

2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, Administrator Systemu powinien uwzględniać dedykowane przyzwolenia dostępu.

II.16. KOMUNIKACJA WEWNĘTRZNA

1. Przesyłanie danych osobowych w komunikacji wewnętrznej (LAN) musi być oznaczone w sposób dostępny jedynie dla uprawnionych użytkowników przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.
2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, użytkownik systemu wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych i w oparciu o przepisy prawne regulujące sposób wysyłania tych danych.

II.17. OZNACZENIE NOŚNIKÓW DANYCH

Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

II.18. BEZPIECZEŃSTWO NOŚNIKÓW, URZADZEŃ

I. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.
2. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
3. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 10 minut nieaktywności użytkownika automatycznie wyłączają możliwość eksploracji ekranu.

II.19 PRZENOSNE NOŚNIKI INFORMATYCZNE

Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie Inspektora o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. Inspektor może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.

II.20 PRZENOSNY KOMPUTER

Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

II.21. WYDRUKI

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu.
2. Wydruki zawierające dane osobowe, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

II.22. DANE UŻYTKOWNIKA

System powinien umożliwić udostępnienie na piśmie, w zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, a w szczególności:

a) daty pierwszego wprowadzenia danych tej osoby,
b) źródła pochodzenia danych,
c) nazwy użytkownika wprowadzającego dane,
d) informacji - komu, kiedy i w jakim zakresie dane zostały udostępnione,
e) sprzeciwu, o którym mowa w art. 32 ust. l pkt 7, po jego uwzględnieniu, oraz sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych.

II.23. ODPOWIEDZIALNOŚĆ

Naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

II.24. OBOWIĄZKI ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) realizacja zadań związanych z przeszkoleniem użytkowników w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali,
2) zapoznanie użytkowników z treścią Instrukcji,
3) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych,
4) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa,
5) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym,
6) zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień ,
7) utrzymanie systemu w należytej sprawności technicznej,
8) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych,
9) Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których przetwarzane są dane osobowe,
10) współpraca z inspektorem w trakcie sprawozdań planowych.