POLITYKA BEZPIECZEŃSTWA

DANYCH OSOBOWYCH

Administrator danych:

nazwa	**Publiczne Przedszkole nr 10**
adres	**Ul. Edukacyjna 13 A**

Dokument:

Data i miejsce zatwierdzenia dokumentu:	Jastrzębie-Zdrój, 1 września 2019 roku
Ilość stron:	21
Zatwierdził:	**DYREKTOR** **Publicznego Przedszkola nr 10** **/-/ Mirosława Lasecka**

1. Wstęp

Administrator Danych wdraża niniejszą Politykę będącą dokumentem opisującym zasady ochrony danych osobowych w celu spełnienia wymagań 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) oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 DZ.U.2018 poz. 1000. Dokument niniejszy stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z ogólnym rozporządzeniem o ochronie danych , a także usprawnienie i usystematyzowanie organizacji pracy w zakresie zapewnienia bezpieczeństwa danych osobowych przetwarzanych przez Administratora danych.

2. Definicje.

W Polityce przyjmuje się następującą terminologię:

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W ramach niniejszego dokumentu jest to Dyrektor Placówki wskazanej jako Administrator.

RODO – ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO 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) 95/46 z 27 kwietnia 2016 r.

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną przez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden oraz więcej czynników specyficznych określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej o których mowa w art. 4 pkt 1 RODO**.**

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 o których mowa w art. 4 pkt 2 RODO.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Anonimizacja - zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych. Jest to proces nieodwracalny.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. przez zastępowanie imienia i nazwiska liczbami lub innymi pseudonimami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym zapewniającym brak dostępu dla osób, które nie mają uprawnień nadanych przez administratora.

Zgoda osoby, której dane dotyczą - oznacza w pełni świadome i dobrowolne oświadczenie lub wyraźne działanie potwierdzające wyrażenie zgody na przetwarzanie danych osobowych przez osobę, której dane dotyczą, przy czym to Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. 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.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo (wykaz rodzajów operacji przetwarzania wymagających oceny skutków opublikowany w Monitorze Polskim), lub w przypadku kiedy ryzyko naruszenia praw i wolności będzie wysokie.

Podmiot danych - osoba fizyczna, której dane dotyczą.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (**procesor)** - osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu Administratora.

Inspektor Ochrony Danych (IOD) - osoba wyznaczona przez Administratora w celu informowania i doradzania Administratorowi w zakresie obowiązującego prawa o ochronie danych oraz w celu monitorowania przestrzegania przepisów o ochronie danych oraz działająca jako punkt kontaktowy dla podmiotów danych, a także organu nadzorczego.

Szczególne kategorie danych osobowych oznaczają informacje na temat pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, stanu zdrowia, kodu genetycznego, nałogów lub życia seksualnego, skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

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

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

Organ nadzorczy – Urząd Ochrony Danych Osobowych.

3. Dane osobowe.

1. Administrator przetwarza dane osobowe gromadzone w zbiorach danych.
2. Dane osobowe domyślnie przetwarzane są na obszarze obejmującym pomieszczenia biurowe, sale lekcyjne i sale zajęć oraz archiwum zlokalizowane w siedzibie administratora. Dodatkowy obszar, w którym przetwarzane są dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym w zdaniu poprzedzającym.

4. Upoważnienia.

1. Administrator upoważnia na piśmie wszystkie osoby, które w związku z realizacją zadań i obowiązków służbowych wykonywanych na polecenie administratora mają dostęp do danych osobowych.
2. Osoby upoważnione oraz wszystkie inne osoby, którym udostępnia się dane osobowe zobowiązane są do przetwarzania danych osobowych zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych regulaminów lub procedur wewnętrznych związanych z przetwarzaniem danych osobowych.
3. Przy zatrudnianiu Pracowników oraz w toku zatrudnienia Administrator zapewnia, że:
   1) Pracownicy przed przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad przetwarzania i ochrony danych osobowych;
   2) Każdy z pracowników zostaje upoważniony na piśmie do przetwarzania danych osobowych dzieci w tym ich rodziców/opiekunów prawnych w zakresie niezbędnym dla właściwej realizacji powierzonych obowiązków służbowych i zadań na czas wykonywania tych obowiązków służbowych i zadań, zgodnie z wzorem stanowiącym **Załączniki nr 1** do Polityki.
   3) Osobom, które mają dostęp do danych osobowych pracowników, w związku z realizacją art. 22^{1b} Kodeksu Pracy nadaje się upoważnienie zgodnie ze wzorem stanowiącym **złącznik nr 2 do Polityki**;
   4) Pracownicy mający dostęp do danych osobowych osób korzystających ze świadczeń w ramach zakładowego funduszu świadczeń socjalnych o których mowa w art. 9 ust. 1 rozporządzenia 2016/679 zgodnie z Art. 8 ust. 1b Ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych, muszą posiadać pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy. Wzór upoważnienia stanowi **załącznik nr 3** do Polityki.
4. Administrator odpowiada za nadawanie upoważnień do przetwarzania danych osobowych.
5. Każda osoba upoważniona może przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.
6. Upoważnienia nadawane są pracownikom, zleceniobiorcom, stażystom, praktykantom oraz innym osobom, które w ramach wykonywania czynności służbowych na rzecz

Administratora mają dostęp do danych osobowych .

7. Nadane upoważnienia do przetwarzania danych osobowych przechowywane są w części B akt osobowych pracownika lub w dokumentacji prowadzonej dla osób wykonujących inne czynności na rzecz administratora (np. dokumentacja praktyk, stażów)
8. Osoba, która przetwarza dane osobowe w systemie informatycznym uzyskuje dostęp do tego systemu poprzez nadanie loginu, jako indywidualnego identyfikatora służącego rozliczalności tego dostępu oraz hasło zabezpieczające.
9. Hasło dostępu należy bezwzględnie chronić i utrzymywać w tajemnicy.
10. Uprawnienie dostępu do systemu informatycznego może uzyskać wyłącznie osoba upoważniona przez administratora do przetwarzania danych osobowych.
11. Loginy podlegają wpisaniu do ewidencji nadanych uprawnień prowadzonej według wzoru stanowiącego **załącznik nr 5 do niniejszej Polityki**.
12. W Ewidencji nadanych uprawnień zamieszcza się następujące informacje: imię i nazwisko osoby uprawnionej, zajmowane stanowisko, loginy do systemów informatycznych, datę nadania loginu oraz datę odebrania loginu .
13. Jeżeli administrator danych prowadził rejestr nadanych upoważnień, w którym rejestrował nadane loginy to dopuszcza się kontynuowanie tego rejestru jako spełniającego wymogi rejestru nadanych uprawnień..

5. Rejestr czynności przetwarzania.

1. Za pośrednictwem rejestru Administrator dokumentuje czynności przetwarzania danych osobowych oraz inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Poprzez wskazanie w rejestrze ogólnych środków ochrony danych osobowych objętych wyodrębnioną czynnością przetwarzania, Administrator dąży również do wykazania zgodności przetwarzania danych osobowych z wymogami prawa.
2. Prowadzenie **rejestru czynności przetwarzania** danych ma na celu zapewnienie zgodności z zasadami i warunkami przetwarzania danych osobowych. Dzięki danym zebranym w tym rejestrze administrator może ocenić, w jakim zakresie dotyczą go inne obowiązki wynikające z RODO np. obowiązek przeprowadzenia oceny skutków przetwarzania dla ochrony danych.
3. Rejestr pozwala zatem na stałą weryfikację działalności w zakresie przetwarzania danych osobowych oraz poddawanie ocenie każdego nowo wprowadzanego lub modyfikowanego procesu już na jego najwcześniejszym etapie.

4. W przypadku podjęcia się przez Administratora zadań procesora i przetwarzania danych osobowych powierzonych przez innych administratorów, Administrator prowadzi dodatkowo **rejestr wszystkich kategorii czynności przetwarzania.**

6. Analiza ryzyka.

1. Administrator musi samodzielnie analizować ryzyko, uwzględniając wiele specyficznych dla niego czynników, takich jak: wielkość, struktura organizacyjna, możliwości techniczne, zakres i rodzaj danych, cel przetwarzania danych.
2. Szacowanie ryzyka to proces ciągły, który powinien być przeprowadzany przy użyciu konkretnej metody, zapewniającej jednocześnie stosowanie jednolitych definicji i pojęć.
3. Administrator danych przeprowadza analizę ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
4. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie zbiorów, które należy zabezpieczyć.
5. Poprzez określenie prawdopodobieństwa oraz skutków wystąpienia danego (niepożądanego) zdarzenia Administrator określa wysokość ryzyka wystąpienia incydentu w danym zbiorze.
6. Po przeprowadzeniu analizy ryzyka Administrator podejmuje określone działania skierowane na obniżenie wpływu ryzyka na funkcjonowanie danego podmiotu i dokonuje wyboru odpowiednich środków przeciwdziałania i minimalizacji ryzyka.
7. Oceniając prawdopodobieństwo wystąpienia danego zdarzenia należy wziąć pod uwagę istniejące mechanizmy kontrolne, ich skuteczność oraz poziom zaawansowania.
8. Identyfikując prawdopodobieństwo wystąpienia zagrożenia Administrator kieruje się doświadczeniem oraz wiedzą na temat incydentów, które wystąpiły w przeszłości w swojej placówce, jak również analizuje możliwość wystąpienia danego zagrożenia na podstawie informacji uzyskanych podczas inwentaryzacji czynności przetwarzania oraz osób, które mają dostęp do przetwarzania danych osobowych.
9. Poziom istotności ryzyka jest iloczynem skali prawdopodobieństwa jego wystąpienia i wartości oszacowanych potencjalnych skutków.

R = P x S

gdzie:

R – poziom istotności ryzyka

P – Prawdopodobieństwo wystąpienia zdarzenia

S – Skala oddziaływania w przypadku wystąpienia zdarzenia (Skutek).

10. Przy ocenie prawdopodobnych skutków wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie;

1 – oznacza skutek nieznaczny,

2 – oznacza skutek mały,

3 – oznacza skutek średni,

4 – oznacza skutek poważny,

5 – oznacza skutek wysoki.

11. Przy ocenie prawdopodobieństwa wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie:

1 – oznacza prawdopodobieństwo bardzo małe (0-20 %),

2 – oznacza prawdopodobieństwo małe (21 - 40%),

3 – oznacza prawdopodobieństwo średnie (41 - 60 %),

4 – oznacza prawdopodobieństwo duże (61 - 80 %),

5 – oznacza prawdopodobieństwo wysokie (81 -100 %).

12. W celu dokonania oceny ryzyka wykorzystuje się mapę istotności ryzyka, która stanowi macierz prawdopodobieństwo-skutek.

Prawdopodobieństwo						
Wysokie	5	10	15	20	25	
Duże	4	8	12	16	20	
Średnie	3	6	9	12	15	
Małe	2	4	6	8	10	
B.małe	1	2	3	4	5	
	Nieznaczny	Mały	Średni	Poważny	Wysoki	Skutek

13. Mapa ryzyka definiuje ryzyka na :
    1) niskie o wartości 4 i mniejszej;
    2) średnie o wartości powyżej 4 i mniejszej niż 15;
    3) wysokie – o wartości powyżej 15.

14. Dla każdego zidentyfikowanego i poddanego analizie ryzyka właściciel ryzyka wskazuje optymalną reakcję, do których zaliczamy:

    1) **Tolerowanie** – w przypadkach, kiedy możliwość przeciwdziałania jest ograniczona lub koszty skutecznego przeciwdziałania ryzyku mogą przekroczyć przewidziane korzyści, a także gdy poziom ryzyka jest akceptowalny;

    2) **Przeniesienie** – dotyczyć to będzie kategorii ryzyk w odniesieniu do których nastąpi przeniesienie ich na inny podmiot np. poprzez ubezpieczenie lub zlecenie usług na zewnątrz;

    3) **Działanie** – dotyczyć to będzie kategorii ryzyk, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań zaradczych w celu zmniejszenia ryzyka do poziomu akceptowalnego lub jego likwidacji;

4) **Wycofanie** – zaniechanie działań powodujących zbyt duże ryzyko.

15. Metoda oceny ryzyka przedstawiona powyżej nie stanowi jedynej, dopuszczonej przez Administratora metody szacowania tego ryzyka

16. Ocena ryzyka dokonywana jako wykaz działań niosących ryzyko dla wolności i praw osób, których dotyczą, przeprowadzona zgodnie z wytycznymi grupy roboczej 29 - wp 248/2017, może mieć również zastosowanie, jeżeli w ocenie Administratora metoda ta pozwoli na ustalenie, czy dane ryzyko jest akceptowalne, czy nie akceptowalne.

7. Zasady ochrony danych.

1. Administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”);
   3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
   4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
   5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”);
   6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

3. Przy zapewnieniu przetwarzania danych osobowych zgodnie z zasadami wskazanymi wyżej Administrator opiera przetwarzanie na następujących podstawach:
   1) Legalność – Administrator dba o ochronę prywatności i przetwarza dane osobowe zgodnie z wymogami prawa;
   2) Bezpieczeństwo − Administrator zapewnia odpowiedni poziom bezpieczeństwa danych osobowych podejmując stale działania w tym zakresie;
   3) Prawa Jednostki − Administrator umożliwia osobom, których dane osobowe przetwarza, wykonywanie swoich praw i prawa te realizuje;
   4) Rozliczalność – Administrator zapewnia należyte udokumentowanie sposobu spełniania obowiązków w zakresie ochrony danych osobowych.

8. Bezpieczeństwo danych osobowych.

Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
1) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
2) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
3) dostosowuje środki ochrony danych do ustalonego ryzyka;
4) posiada system zarządzania bezpieczeństwem informacji;
5) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami;
6) dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających;
7) wprowadza regulaminy i instrukcje postępowania z danymi osobowymi.

9. Zadania oraz status Inspektora Ochrony Danych.

1. Do zadań Inspektora ochrony danych należy w szczególności:
   1) informowanie Dyrektora oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach wynikających z rozporządzenia RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach;

2) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego 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, tj. Urzędem Ochrony Danych Osobowych;

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. Administrator publikuje na swojej stronie internetowej dane Inspektora Ochrony Danych, tj. imię i nazwisko oraz adres e-mail do kontaktu.

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

4. Administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

5. Administrator wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania.

6. Administrator zapewnia, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania swoich zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora.

7. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

8. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.

9. Jeżeli Inspektor ochrony danych miałby wykonywać inne zadania i obowiązki, niż wymienione w ust. 1 to Administrator zapewnia, by te zadania i obowiązki nie powodowały konfliktu interesów.
10. Wyznaczenie inspektora ochrony danych może nastąpić w formie bezpośredniego wskazania w umowie zawartej z podmiotem zewnętrznym w celu wykonywania tych zadań, w zakresie czynności, jeżeli zadania podejmuje się pracownik. Można zastosować dokument wyznaczenia inspektora według wzoru stanowiącego **załącznik nr 7** do Polityki.

10. Postępowanie z incydentami oraz naruszeniami ochrony danych osobowych

Postępowanie Administratora danych osobowych lub osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia zagrożenia:

1) ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków,
2) w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,
3) w razie konieczności zainicjowanie działań dyscyplinarnych,
4) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
5) udokumentowanie prowadzonego postępowania w rejestrze incydentów i naruszeń bezpieczeństwa danych osobowych zgodnie ze wzorem stanowiącym **załącznik nr 6** do niniejszej Polityki.

Administrator opracowuje szczegółową instrukcję postępowania na wypadek wystąpienia zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych oraz w przypadku naruszenia.

11. Szkolenia

1. Osoby zatrudnione w obszarze przetwarzania (w szczególności pracownicy administracji, nauczyciele) przed dopuszczeniem do pracy z danymi osobowymi powinny być zapoznane przez Administratora z niniejszą Polityką bezpieczeństwa danych osobowych oraz zobowiązane do zachowania w tajemnicy przetwarzanych przez siebie danych osobowych w trakcie zatrudnienia jak i po jego ustaniu.

2. Osoby zatrudnione w obszarze przetwarzania (w szczególności pracownicy administracji, nauczyciele) przed dopuszczeniem do pracy z danymi osobowymi powinny zapoznać się z informacjami zawartymi w karcie instruktażu wstępnego stanowiącej **załącznik nr 4 do Polityki.**

   Kartę szkolenia wstępnego należy przechowywać w części B akt osobowych pracownika lub dokumentacji prowadzonej dla osoby upoważnionej (dokumentacja praktyk, stażów).
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych przez Inspektora Ochrony Danych, wskazane jest udokumentowanie odbycia tego szkolenia.
4. Wewnętrzne szkolenie przypominające zostaje zakończone podpisaniem przez pracownika listy uczestników szkolenia.

12. Audyty

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. Audyt przeprowadza Inspektor Ochrony Danych wraz z pracownikiem wyznaczonym przez Administratora.

13. Wykaz podstawowych zabezpieczeń stosowanych przez Administratora danych:

a. Środki organizacyjne:

1. Opracowano i wdrożono Politykę bezpieczeństwa danych osobowych.
2. Do przetwarzania danych dopuszczono wyłącznie osoby posiadające upoważnienia nadane przez Administratora Danych.
3. Prowadzona jest ewidencja osób uprawnionych do dostępu do systemów informatycznych.
4. Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych.
5. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy.
6. Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
7. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
8. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
9. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
10. Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami (procesorami) przetwarzającymi dane osobowe.
11. W każdym przypadku budzącym wątpliwości co do legalności udostępnienia danych osobowych podmiotowi upoważnionemu do otrzymania Administrator udostępnia dane wyłącznie na pisemny wniosek tego podmiotu.
12. W podmiocie prowadzi się politykę czystego biurka.
13. Wdrożono procedurę (instrukcję) otwierania i zamykania budynków oraz pomieszczeń biurowych, z którą zapoznaje się odpowiedzialnych za tę czynność pracowników.

b. Środki ochrony fizycznej danych

1. Dane osobowe przechowywane są w pomieszczeniach zamykanych na klucz.
2. Jeżeli zbiór danych osobowych przechowywany jest w pomieszczeniu na parterze, to okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
3. Dane osobowe w formie papierowej są przechowywane w zamkniętych niemetalowych lub metalowych szafach.
4. Po zakończeniu pracy, przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w zamykanych szafach bądź biurkach.
5. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie.
6. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
7. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

c. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. Dostęp do internetu oraz sieci lokalnej zabezpieczony jest hasłem.
2. Zastosowano urządzenia typu UPS chroniący system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
3. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
5. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
6. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
7. Użyto system Firewall do ochrony dostępu do sieci komputerowej.

d. Środki ochrony w ramach narzędzi programowych i baz danych

1. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zastosowano kryptograficzne środki ochrony danych osobowych.
3. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
4. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

14. Polityka czystego biurka

1. Polityka czystego biurka obowiązuje wszystkich pracowników, przy czym za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy.
2. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.
3. Każdy Pracownik zobowiązany jest do ograniczenia dostępu osób postronnych do danych poufnych, w tym danych osobowych zawartych na nośnikach papierowych wykorzystywanych przez Pracownika przy wykonywaniu obowiązków służbowych.
4. W przypadku opuszczenia przez pracownika – choćby chwilowo – biurka lub stanowiska pracy Pracownik zobowiązany jest do odłożenia i schowania wszystkich wykorzystywanych dokumentów zawierających dane poufne lub dane osobowe do zamykanej szuflady lub szafy, celem uniemożliwienia dostępu do dokumentów osobom postronnym.
5. Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu.
6. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej na klucz szafy.
7. Po zakończonej pracy na biurku mogą znajdować się jedynie telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis, itp.
8. Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.

15. Prawa osób, których dane dotyczą

1. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności, takich jak zgłoszenie sprzeciwu lub ograniczenie przetwarzania.
2. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane osobowe przetwarza.
3. Administrator publikuje na swojej stronie internetowej , oraz pozostawia do wglądu w siedzibie:
    1) Informację o prawach osób, których dane dotyczą;
    2) Informację o zakresie przetwarzanych danych osobowych w poszczególnych celach;
    3) Metodach kontaktu z Administratorem w zakresie danych osobowych.
4. W celu realizacji praw osoby, której dane osobowe dotyczą Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.
5. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób, informując osobę, której dane dotyczą o:
    1) przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby;
    2) przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej;
    3) planowanej zmianie celu przetwarzania danych;
    4) przed uchyleniem ograniczenia przetwarzania;
    5) sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba, że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe);
    6) prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
6. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

7. Niezależnie od postanowień ust. 5 wyżej, Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe poprzez wywieszenie informacji o objęciu obszaru monitoringiem wizyjnym.

8. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

9. Administrator wydaje osobie, której dane osobowe dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

10. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której dane osobowe dotyczą. Administrator ma prawo odmówić sprostowania danych chyba, że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga.

11. Administrator uzupełnia i aktualizuje dane na żądanie osoby, której dane osobowe dotyczą. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby, co do uzupełnianych danych chyba, że będzie to niewystarczające w świetle przyjętych przez Administratora procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

12. Z uwzględnieniem ust. 13 niżej, na żądanie osoby, Administrator usuwa dane, gdy:

1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
4) dane były przetwarzane niezgodnie z prawem,
5) konieczność usunięcia wynika z obowiązku prawnego,
6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

13. Administrator przy usuwaniu danych osobowych uwzględnia, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

14. Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

1) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

3) Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

4) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

15. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą chyba, że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

16. Procedura (instrukcja) obsługi żądań podmiotów danych jest dokumentem, z którym Administrator zapoznaje pracowników odpowiedzialnych za tę czynność.

16. Postanowienia końcowe.

1. Polityka jest przechowywana i udostępniana w wersji papierowej oraz elektronicznej w siedzibie Administratora.
2. Administrator w uzupełnieniu do niniejszej Polityki bezpieczeństwa danych osobowych , w celu uszczegółowienia niektórych procedur w niej zawartych, opracowuje i udostępnia do zapoznania się przez pracowników wyznaczonych do realizowania tych procedur, instrukcje określające szczegółowe zasady postępowania.
3. **Wdrożenie odrębnych instrukcji dotyczących procedur w zakresie przetwarzania danych osobowych nie wymaga wprowadzenia zarządzeniem dyrektora jednostki**.
4. **Dopuszcza się prowadzenie rejestrów (np. rejestr nadanych uprawnień, rejestr naruszeń) w wersji elektronicznej.**
5. Polityka niniejsza wchodzi w życie z mocą obowiązującą od 1 września 2019 roku.
6. **Załączniki do Polityki:**

Nr załącznika	Opis załącznika
Załącznik nr 1	Wzór upoważnienia do przetwarzania danych osobowych uczniów
Załącznik nr 2	Wzór upoważnienia do danych osobowych pracowników
Załącznik nr 3	Wzór upoważnienia do danych osobowych w ramach zfśs
Załącznik nr 4	Karta szkolenia wstępnego z zakresu ochrony danych osobowych
Załącznik nr 5	Wzór ewidencji nadanych uprawnień
Załącznik nr 6	Wzór rejestru incydentów i naruszeń bezpieczeństwa danych osobowych
Załącznik nr 7	Wzór wyznaczenia IOD