Polityka Bezpieczeństwa Ochrony Danych Osobowych Szkoły Podstawowej nr 31 z Oddziałami Integracyjnymi im Henryka Sienkiewicza w Kielcach

POLITYKA OCHRONY DANYCH OSOBOWYCH

Administrator Danych – Dyrektor Szkoły

dnia 24.05.2018 r. w podmiocie o nazwie:

Szkoła Podstawowa nr 31 z Oddziałami Integracyjnymi im Henryka Sienkiewicza w Kielcach ul. Krzemionkowa 1 3; 25-750 Kielce

zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

wdraża dokument o nazwie „Polityka Ochrony Danych Osobowych". Postanowienia tego dokumentu wchodzą w życie z dniem 25.05.2018 r.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych (dalej „Polityka") w podmiocie: określa zasady przetwarzania danych osobowych, oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych, oraz w systemach informatycznych. Niniejsza Polityka bezpieczeństwa przetwarzania danych osobowych została wdrożona w Szkoła Podstawowa nr 31 z Oddziałami Integracyjnymi im Henryka Sienkiewicza w Kielcach i opisuje szczegółowe zasady i procedury ochrony i nadzoru nad przetwarzaniem danych osobowych.

Każde naruszenie zasad Polityki może być uznane za poważne naruszenie podstawowych obowiązków pracowniczych lub wynikających z umów cywilnych o współpracy i może skutkować konsekwencjami, zgodnie z Kodeksem Pracy lub odpowiednimi przepisami regulującymi zasady współpracy, jak również odpowiedzialnością przewidzianą w ustawie o ochronie danych osobowych.
W celu zapewnienia bezpieczeństwa przetwarzanych danych wymaga się, aby wszyscy jego użytkownicy byli świadomi konieczności ochrony wykorzystywanych zasobów. Konsekwencją nie stosowania przez pracownika środków bezpieczeństwa określonych w instrukcjach wewnętrznych może być zniszczenie części lub całości systemów informatycznych, utrata poufności, autentyczności, straty finansowe, jak również utrata wizerunku.

Spis treści

Informacje ogólne:

a. Administratorem Danych w Szkole Podstawowej nr 31 z Oddziałami Integracyjnymi im Henryka Sienkiewicza w Kielcach NIP: 9591577462 jest Dyrektor Szkoły Pani Mgr Marta Dibelka.
b. Szkoła działa na podstawie Ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U z 2004 r. Nr 256, poz 2572, z późn. zm. (Dz. U. z 2017 r. poz. 2198, 2203 i 2361)).

Terminologia:

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań,
Dane wrażliwe - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących odpowiedzialności karnej, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym,
Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
Administrator danych (ADO) – Szkoła Podstawowa nr 31 z Oddziałami Integracyjnymi im Henryka Sienkiewicza w Kielcach (jednostka organizacyjna), reprezentowany przez Dyrektora placówki, który decyduje o celach i środkach przetwarzania danych osobowych,
Administrator ochrony systemu informatycznego (ASI) rozumie się osobę odpowiedzialną za funkcjonowanie systemu informatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w systemie,
Inspektor Ochrony Danych (IOD) – osoba lub podmiot wyznaczony przez ADO, nadzorujący przestrzeganie zasad ochrony danych osobowych
Przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
Nośniki danych osobowych – dyskietki, płyty CD lub DVD, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi,
Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
Haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
Odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą,

Osobie upoważnionej do przetwarzania danych osobowych - rozumie się przez to pracownika szkoły, która upoważniona została na piśmie do przetwarzania danych osobowych przez dyrektora szkoły
Uwierzytelnianiu -rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu
Użytkowniku - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło,
Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Poufność – oznacza zapewnienie, że informacja nie jest udostępniana lub ujawniana / nieupoważnionym osobom, podmiotom lub procesom.
Dostępność – oznacza zapewnienie osiągalności lub możliwości do wykorzystania na żądanie, w założonym czasie przez uprawniony podmiot.
Autentyczność – oznacza zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów).
Niezaprzeczalność – oznacza zapewnienie braku możliwości wyparcia się swojego uczestnictwa w całości lub w części przetwarzania danych przez jeden z podmiotów uczestniczących w przetwarzaniu

Sposób przechowywania, udostępniania i modyfikacji Polityki

Polityka została zatwierdzona w Podmiocie Administratora danych jako dokument obowiązujący.

Niniejszy dokument jest przechowywany i aktualizowany w wersji elektronicznej i papierowej ze względu na czytelność i różnorodność obszarów, w których przetwarzane są dane osobowe. Jest on regularnie przeglądany i aktualizowany przez Administratora Danych oraz przez Inspektora Ochrony Danych.

Zmiany w dokumencie Polityki oraz załącznikach wprowadzane są w chwili pojawienia się ważnych okoliczności lub nowego przepisu, istotnego dla spójności i aktualności Polityki, bądź aktualizacji dotychczasowych przepisów dotyczących ochrony lub przetwarzania danych osobowych. Zmiany zatwierdzane są przez Administratora Danych.

Informacje o zmianach podawane są do wiadomości osób uczestniczących w przetwarzaniu danych osobowych poprzez publikację w intranecie lub dokumentach formalnych udostępnianych w ustalony wewnętrznie sposób.

W przypadku zatwierdzenia nowej wersji Polityki jest ona drukowana, a wydruk dołączany jest do prowadzonej dokumentacji ochrony danych osobowych. Załączniki mogą być przechowywane wyłącznie w formie elektronicznej. Ich wydruk następuje tylko w razie zaistnienia takiej konieczności, na zlecenie Administratora Danych lub Inspektora Ochrony Danych.

Dokument Polityki, wraz z załącznikami, stanowi tajemnicę Podmiotu Administratora Danych i jest klasyfikowany jako dokument wewnętrzny.

Zmiany i udostępnianie tekstu Polityki

1. Dopuszcza się dokonywanie zmian w niniejszym dokumencie oraz dokumentach powiązanych tylko przez osoby upoważnione, na zasadach opisanych w Polityce.
2. Tekst niniejszej Polityki wraz z załącznikami zostanie udostępniony osobom przetwarzającym dane w intranecie Administratora danych, aby mogły się one z nim zapoznać i postępować zgodnie z jej postanowieniami.

Znajomość Polityki

Do zapoznania się z niniejszym dokumentem Polityki oraz stosowania zawartych w niej zasad zobowiązane są wszystkie osoby przetwarzające dane osobowe w jednostce/firmie

Strategia bezpieczeństwa i zasady przetwarzania danych.

Analiza ryzyka i uzasadnienie dla zastosowania określonych założeń bezpieczeństwa danych osobowych.

Ankieta ryzyka

Pytania dotyczące charakteru przetwarzanych danych osobowych:

Czy przetwarzanie może skutkować:	BRAK RYZYKA	ZNIKOME RYZYKO	ŚREDNIE RYZYKO	WYSOKIE RYZYKO
Dyskryminacją		X		
kradzieżą tożsamości lub oszustwem dotyczącym tożsamości		X		
stratą finansową		X		
naruszeniem dobrego imienia		X		
naruszeniem poufności danych osobowych chronionych tajemnicą zawodową		X		
wszelką inną znaczną szkodą gospodarczą lub społeczną		X		

Pytania dotyczące kwestii organizacyjno-technicznych:

Czy w odniesieniu do przetwarzanych danych osobowych:	BRAK RYZYKA	ZNIKOME RYZYKO	ŚREDNIE RYZYKO	WYSOKIE RYZYKO
istnieje ryzyko dostępu osób trzecich do dokumentacji papierowej zawierającej dane osobowe w godzinach pracy szkoły		X		
istnieje ryzyko dostępu osób trzecich do dokumentacji elektronicznej zawierającej dane osobowe w godzinach pracy szkoły		X		
istnieje ryzyko dostępu osób trzecich do dokumentacji papierowej zawierającej dane osobowe poza godzinami pracy szkoły		X		
istnieje ryzyko dostępu osób trzecich do		X		

dokumentacji elektronicznej zawierającej dane osobowe poza godzinami pracy szkoły				
istnieje ryzyko wyniesienia dokumentacji zawierającej dane osobowe poza budynek szkoły		X		
istnieje ryzyko skopiowania przez osobę trzecią dokumentów zawierających dane osobowe przetwarzane w szkole		X		
istnieje ryzyko kradzieży dokumentów zawierających dane osobowe przetwarzane w szkole		X		
istnieje ryzyko zagubienia dokumentów zawierających dane osobowe przetwarzane w szkole		X		
istnieje ryzyko stosowania przez osoby trzecie podsłuchu bezpośredniego lub akustycznego z wykorzystaniem mikrofonów kierunkowych lub instalacji technicznych		X		
istnieje ryzyko zagubienia elektronicznych nośników danych zawierających dane osobowe przetwarzane w szkole		X		

Pytania dotyczące zabezpieczenia sprzętu elektronicznego:

Czy w odniesieniu do przetwarzanych danych osobowych:	BRAK RYZYKA	ZNIKOME RYZYKO	ŚREDNIE RYZYKO	WYSOKIE RYZYKO
istnieje ryzyko włamania do systemu poprzez podszycie się pod uprawnionego użytkownika		X		
istnieje ryzyko nieuprawnionego instalowania urządzeń służących do naruszenia poufności przetwarzanych		X		
istnieje ryzyko nieuprawnionej, świadomej modyfikacji oprogramowania zainstalowanego na komputerze pracownika przez osoby trzecie		X		
istnieje ryzyko użycia oprogramowania zainstalowanego na komputerach pracowników w nieuprawniony sposób		X		
istnieje ryzyko korzystania z nielicencjonowanego		X		

oprogramowania na komputerach pracowników				
istnieje ryzyko przeglądania (przeszukiwania) pamięci operacyjnej i zewnętrznej komputerów w celu uzyskania określonych informacji		X		
istnieje ryzyko wykorzystania pozostawionych na dysku twardym komputera plików roboczych wytworzonych przez oprogramowanie		X		
istnieje ryzyko skopiowania/kradzieży danych osobowych podczas wykonywania napraw i konserwacji komputerów		X		
istnieje ryzyko przypadkowej zmiany ustawień konfiguracyjnych na komputerach		X		
istnieje ryzyko nieupoważnionego uruchomienia komputera z nośnika zewnętrznego (ominięcie mechanizmów bezpieczeństwa systemu operacyjnego i systemu plików NTFS i odczytanie zawartości przetwarzanych dokumentów)		X		

Szacowanie poziomu ryzyka

$$\text{Poziom ryzyka} = \frac{0\text{xBR} + 0{,}5\text{xZR} + 1\text{xŚR} + 1{,}5\text{xWR}}{\text{liczba czynników ryzyka}} = 0{,}5$$

gdzie: BR – brak ryzyka, ZR – znikome ryzyko, ŚR – średnie ryzyko, WR – wysokie ryzyko

Skala oceny:

0 - 0,25 – brak ryzyka
0,26 – 0,75 – znikome ryzyko
0,76 – 1,25 – średnie ryzyko
1,26 - 1,5 – wysokie ryzyko

Wnioski:

Ogólny poziom ryzyka związanego z przetwarzaniem danych osobowych oszacowany został:

1) Dla postępowań dotyczących charakteru przetwarzanych danych osobowych – **poziom 0,5**
2) Dla postępowań dotyczących kwestii organizacyjno-technicznych – **poziom 0,5**
3) Dla postępowań dotyczących zabezpieczenia sprzętu elektronicznego – **poziom 0,5**

Najważniejsze ryzyko związane z naruszeniem bezpieczeństwa danych osobowych związane jest z przetwarzaniem danych osobowych w zakresie postępowań prowadzonych w przedmiocie: **Dla postępowań dotyczących zabezpieczenia sprzętu elektronicznego** - Związane jest to przede wszystkim z charakterem przetwarzanych danych, sposobem przetwarzania danych przez personel oraz obsługą systemu informatycznego.
Najważniejszymi obszarami wymagającymi weryfikacji celem minimalizacji poziomu ryzyka są: **usystematyzowanie kwestii organizacyjno-technicznych oraz zabezpieczenia sprzętu elektronicznego dla zwiększenia ochrony danych przechowywanych w systemie informatycznym.**

Po przeprowadzeniu ankiety ryzyka i oszacowaniu poziomu ryzyka proponuje się podjęcie działań w zakresie zwiększenia bezpieczeństwa danych osobowych przetwarzanych w Szkole Podstawowej nr 31 z Oddziałami Integracyjnymi im Henryka Sienkiewicza w Kielcach poprzez:

	Nazwa	Konieczność	Brak konieczności
1	Wprowadzenie dodatkowych zabezpieczeń w zakresie organizacyjno-technicznym		X
2	Wprowadzenie dodatkowych zabezpieczeń komputerów poprzez wprowadzenie haseł do sieci wewnętrznej.		X
3	Zakup nowego oprogramowania antywirusowego do komputerów.		X
4			

Standardy zabezpieczeń stosowanych:

Zabezpieczenia techniczno-organizacyjne budynku i pomieszczeń:

LP	**Zabezpieczenie**	**Występowanie**
1	System alarmowy z monitoringiem i interwencją fizyczną;	1
2	Całodobowy dozór lokalny;	1
3	Drzwi przeciwwłamaniowe z certyfikatem;	0
4	Kraty, rolety przeciwwłamaniowe w oknach;	1

5	System alarmowy;	1
6	Zamki do pomieszczeń z certyfikatem;	0
7	Blokady antywłamaniowe;	0
8	Firma ochrony zewnętrznej – grupa interwencyjna	1

Zabezpieczenia techniczno-organizacyjne szaf zawierających dokumentację:

LP	**Zabezpieczenie**	**Występowanie**
1	Szafy zamykane na klucze;	1
2	Zabezpieczenie szaf zamkami z szyfrem;	1

Zabezpieczenia komputerów:

LP	**Zabezpieczenie**	**Występowanie**
1	Program Antywirusowy	1
2	Zabezpieczenia użytkowników w postaci loginów i haseł dostępowych.	1
3		

Procedury i sposoby zagwarantowania realizacji praw osób, których dane są przetwarzane

Procedura realizacji prawa dostępu do swoich danych osobowych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa dostępu do swoich danych przetwarzanych przez Administratora.

Każdej osobie fizycznej przysługuje prawo do uzyskania wyczerpujących informacji od Administratora, w postaci potwierdzenia, czy dane są faktycznie przetwarzane przez Administratora.

Prawo dostępu do danych osobowych jest realizowane poprzez wydanie kopii przetwarzanych danych osobie, której dane dotyczą.

2. Prawa osoby fizycznej, której dane są przetwarzane

Osoba fizyczna, której dane są przetwarzane ma prawo do uzyskania od Administratora następujących informacji:

a) celach, w jakich przetwarzane są dane osobowe;

b) kategoriach danych osobowych, które podlegają przetwarzaniu;

c) odbiorcach lub kategoriach odbiorców;

d) planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania okresu przechowywania danych;

e) prawie do żądania sprostowania swoich danych osobowych;

f) prawie do usunięcia lub ograniczenia przetwarzania danych osobowych;

g) prawie do wniesienia sprzeciwu wobec konkretnego przetwarzania swoich danych;

h) prawie do wniesienia skargi do organu nadzorczego, na przetwarzanie swoich danych, jeśli są one przetwarzane niezgodnie z obowiązującymi przepisami;

i) w sytuacji, gdy dane osobowe nie zostały zebrane od osoby, której one dotyczą - wszelkich dostępnych informacje o źródle, z którego administrator pozyskał te dane

j) zautomatyzowanym podejmowaniu decyzji, jeżeli takie administrator realizuje wobec konkretnej osoby fizycznej taki sposób przetwarzania, w tym informacji o profilowaniu (art. 22 ust. 1 i 4 RODO), jak również wszelkie istotne informacje o zasadach podejmowania takich decyzji oraz o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby fizycznej, której przetwarzane dane i decyzje dotyczą.

3. Realizacja uprawnienia dostępu do danych

Każda osoba której dane są przetwarzane, ma prawo do wystąpienia do administratora z wnioskiem o wydanie jej informacji o tym, czy dane są przetwarzane, a jeżeli tak, to do uzyskania dostępu do tych danych lub uzyskania ich kopii.

Na wniosek złożony droga elektroniczną, administrator udziela odpowiedzi również drogą elektroniczną.

Pierwsza kopia i jej przekazanie odbywa się bezpłatnie. Za każdą kolejną kopię, o którą zwróci się podmiot danych, Administrator będzie miał prawo pobrać „ opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych" (art. 15 ust. 3 RODO) związanych z jej wytworzeniem (według stawek obowiązujących u Administratora). Umożliwienie wglądu do danych konkretnej osobie fizycznej nie może powodować naruszenia praw innych osób lub też tajemnic prawnie chronionych.

Uzyskując wgląd do swoich danych osoba fizyczna nie może mieć nieuzasadnionego dostępu do danych innych osób fizycznych, lub do danych stanowiących tajemnicę przedsiębiorstwa. W przypadku, gdy przetwarzana jest duża ilość informacji o osobie, która chce skorzystać z prawa dostępu do swoich danych, Administrator kieruje do tej osoby żądanie sprecyzowania do jakich konkretnie danych lub też informacji o czynnościach przetwarzania jej danych chciałaby ona uzyskać dostęp.

4. Terminy na udzielenie odpowiedzi na żądanie:

1) Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie miesiąca od otrzymania tego żądania.

2) Jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań, administrator może wydłużyć czas udzielenia odpowiedzi o kolejne 2 miesiące, zobowiązany jest podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

3) W przypadku, gdy administrator nie zamierza udzielić odpowiedzi oraz podjęcia działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sądu.

Wzór odpowiedzi na skierowany wniosek:

Na podstawie art. 15 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Administrator potwierdza, że Pana/Pani dane osobowe są przetwarzane i jednocześnie informuje, że:

1. Celem przetwarzania Pani/Pana danych osobowych jest ……..;

2. (Administrator) przetwarza Pani/Pana dane osobowe w zakresie ……. (należy wskazać kategorię danych osobowych);

3. Dane osobowe będą ujawniane …….. *(należy wskazać odbiorcę lub kategorie odbiorców);*

Dane osobowe będą przechowywane przez okres ……;

Przysługuje Panu/Pani prawo do sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, a także prawo do wniesienia sprzeciwu oraz skargi do organu nadzorczego;

(Administrator) uzyskał Pani/Pana dane osobowe z …….. (należy wskazać źródło, o ile dane nie zostały pozyskane od osoby, której dotyczą);

(należy dodać informacje dotyczące zautomatyzowanego podejmowania decyzji, w tym profilowania, o ile znajduje to zastosowanie).

……

(data, podpis)

Procedura realizacji prawa do sprostowania/uzupełnienia swoich danych osobowych

1. **Cel procedury**

Celem procedury jest realizacja uprawnienia osoby fizycznej do sprostowania/uzupełnienia swoich danych przetwarzanych przez Administratora.

2. **Prawa osoby fizycznej, której dane są przetwarzane**

Każdej osobie fizycznej przysługuje jednakowe prawo do niezwłocznego sprostowania/uzupełnienia dotyczących go danych osobowych, które są nieprawidłowe lub nieaktualne. Uwzględniając cele przetwarzania, osoba, której dane dotyczą ma prawo do żądania od Administratora uzupełnienia niekompletnych danych osobowych, poprzez przedstawienie odpowiedniego oświadczenia Administratorowi.

Jeżeli osoba fizyczna zażąda uzupełnienia katalogu dotyczących go danych osobowych o te, które nie są niezbędne Administratorowi do działania, to taki wniosek/oświadczenie woli nie musi zostać pozytywnie rozpatrzony przez Administratora dla osoby, której dane dotyczą.

3. **Procedura rozpatrywania żądań o sprostowanie danych osobowych**

Komunikacja z osobą, której dane dotyczą powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i dostępnej formie.

Osoba składająca oświadczeni e/wniosek o sprostowani e/uzupełnienie danych osobowych oświadcza, że jest osobą możliwą do zidentyfikowania, na podstawie dobrowolnie podanych danych osobowych, umożliwiających jej jednoznaczną identyfikację.

W przypadku, gdy Administrator nie jest w stanie zidentyfikować osoby składającej oświadczenie/wniosek o sprostowanie/uzupełnienie danych osobowych, ma prawo na podstawie obowiązujących przepisów prawa odmówić rozpatrzenia żądania, uprzednio podejmując wszelkie możliwe środki w celu zidentyfikowania osoby, która z nim wystąpiła.

Działania podejmowane na podstawie żądania o sprostowanie lub uzupełnienie danych są zwolnione z opłat (art. 12 ust. 5 RODO), lecz jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne (np. ze względu na swój ustawiczny charakter) Administratorowi przysługują dwa uprawnienia:

1) pobranie rozsądnej opłaty, która uwzględnia administracyjne koszty prowadzenia komunikacji i podjętych działań (według stawek obowiązujących u Administratora),

2) odmowa podejmowania działań.

Administrator, w przypadku podjęcia decyzji, o nieuzasadnionym lub nadmiernym charakterze żądania ma obowiązek wykazania takich cech żądania (wniosku) w ewentualnym postępowaniu przed organem nadzorczym.

Administrator jest zobowiązany po dokonaniu sprostowania/ uzupełnienia danych osobowych poinformować wszystkich odbiorców którym ujawniono dane podlegające uzupełnieniu/sprostowaniu o fakcie ich uzupełnienia/sprostowania.

W przypadku braku możliwości wykonania powyższego, lub gdy działanie takie wymagałoby niewspółmiernie dużego wysiłku ze strony Administratora, może on podjąć decyzję o nieudzieleniu stosownej informacji odbiorcom, jednakże ma obowiązek wykazania braku tej możliwości lub niewspółmiernie dużego wysiłku w ewentualnym postępowaniu przed organem nadzorczym**.**

4. **Terminy rozpatrywania żądań o sprostowanie/uzupełnienie danych osobowych.**

Na podstawie art. 12 ust. 3 RODO, Administrator podejmuje decyzję o przyjęciu/odrzuceniu oświadczenia/wniosku o sprostowanie/uzupełnienie danych osobowych bez zbędnej zwłoki.

5. **Terminy na udzielenie odpowiedzi na żądanie:**

1) Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie miesiąca od otrzymania tego żądania;

2) Jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań, administrator może wydłużyć czas udzielenia odpowiedzi o kolejne 2 miesiące, jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

3) W przypadku, gdy Administrator nie zamierza udzielić odpowiedzi i działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości **wniesienia sprawy do sądu.**

Procedura realizacji prawa do usunięcia swoich danych osobowych

1. **Cel procedury**

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa usunięcia swoich danych osobowych („prawo do bycia zapomnianym") przetwarzanych przez Administratora.

2. **Prawa osoby fizycznej, której dane są przetwarzane**

Każdej osobie fizycznej przysługuje jednakowe prawo żądania usunięcia jego danych osobowych przetwarzanych przez Administratora.

Składa się ono z następujących uprawnień:

1) możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez Administratora danych,

2) możliwości żądania, aby Administrator danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by ci administratorzy usunęli wszelkie łącza do tych danych lub ich kopie, czy ich replikacje.

Obowiązek poinformowania innych administratorów danych może być ograniczony przez:

a) dostępną technologię,

b) koszty,

c) konieczność ograniczenia się Administratora do „rozsądnych działań".

Administrator, w przypadku podjęcia decyzji, o ograniczeniu poinformowania innych administratorów danych ma obowiązek wykazania takich ograniczeń w ewentualnym postępowaniu przed organem nadzorczym.

3. **Każdemu podmiotowi danych przysługuje jednakowe prawo do „bycia zapomnianym."**

Prawo to można wykonać, jeżeli spełniona jest choć jedna z następujących przesłanek:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

2) osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych;

3) osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych;

4) dane osobowe były przetwarzane w sposób „niezgodny z prawem";

5) dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator";

6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

W przypadku wykonania prawa do bycia zapomnianym, Administrator zaprzestaje przetwarzania danych osobowych i usuwa dane osoby, która złożyła stosowne oświadczenie/ wniosek, chyba że zachodzą szczególne przypadki ograniczające prawo do bycia zapomnianym:

a) istnieje przepis prawa, który nakazuje przetwarzanie danych osobowych,

b) istnieje sytuacja, w której przetwarzanie jest niezbędne do ustalenia dochodzenia lub obrony roszczeń.

Procedura realizacji prawa do przenoszenia swoich danych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do przeniesienia swoich danych osobowych przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Prawo do przenoszenia danych może być wykonane wyłącznie wtedy, gdy osoba, której dane dotyczą uprzednio dostarczyła Administratorowi dane jej dotyczące, lub wyraziła zgodę na pozyskanie przez Administratora tych danych, w inny sposób, określony uprzednio odpowiednim oświadczeniem.

Prawo do przenoszenia danych to, w szczególności prawo do:

1) otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła administratorowi;

2) prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła administratorowi, innemu administratorowi, bez przeszkód ze strony administratora danych, o ile jest to technicznie możliwe.

Prawo do przeniesienia danych może zostać wykonane, gdy:

1) przetwarzanie danych odbywa się na podstawie zgody osoby, lub w celu wykonania umowy;

2) przetwarzanie danych odbywa się w sposób zautomatyzowany - prawo do przenoszenia danych obejmuje tylko te dane osobowe, które są przetwarzane przy użyciu systemów informatycznych i nie obejmuje ono tradycyjnych, manualnych papierowych zbiorów danych.

Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo i które to dane ta osoba dostarczyła Administratorowi. Wykonywanie tego prawa nie może ono niekorzystnie wpływać na praw i wolności innych osób.

Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Procedura realizacji prawa do sprzeciwu

1. **Cel procedury**

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do sprzeciwu do przetwarzania swoich danych osobowych przez Administratora.

2. **Prawa osoby fizycznej, której dane są przetwarzane**

Każda osoba, której Dane są przetwarzane może w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych.

W razie wniesienia takiego sprzeciwu administrator nie może dalej przetwarzać Danych osoby, która wniosła sprzeciw, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych, podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, która wniosła sprzeciw.

W przypadku przetwarzania Danych do celów marketingu bezpośredniego, osoba, której Dane są przetwarzane ma prawo wnieść sprzeciw wobec przetwarzania jej Danych w tym celu. Powyższe dotyczy również sprzeciwu wobec profilowania. Administrator jest zobowiązany poinformować osobę o ww. przysługującym jej uprawnieniu najpóźniej przy okazji pierwszego kontaktu, przy czym wspomniana informacja powinna być przedstawiona w sposób wyraźny i łatwy do zrozumienia - odrębnie od innych informacji.

Szczególne uprawnienia związane z procesami zautomatyzowanego przetwarzania danych - w tym z profilowaniem.

Profilowanie to szczególny rodzaj przetwarzania danych osobowych, który:

- odbywa się w sposób automatyczny,
- ma na celu ocenę osoby fizycznej lub przewidywanie jej zachowania.
- Profilowanie zawsze wymaga poinformowania (w sposób możliwy do zweryfikowania) o nim osób, które są profilowane.

Profilowanie może być wykorzystywane jako narzędzie dla tzw. automatycznego podejmowania decyzji Administratora wobec osób, których dane dotyczą.

Jeżeli takie automatyczne podejmowanie decyzji wywołuje skutki prawne wobec osób, których dane dotyczą, lub w podobny istotny sposób wpływa na te osoby, Administrator może mechanizm ten stosować wyłącznie wtedy, gdy spełniony jest jeden z następujących warunków:

1) osoba profilowana wyrazi na to wyraźną zgodę,
2) profilowanie jest niezbędne do zawarcia lub wykonywania umowy z tą osobą,
3) profilowanie jest dopuszczalne przez szczególne przepisy prawa.

Jeżeli profilowanie miałoby się odbywać w oparciu o szczególne kategorie danych osobowych, wówczas jedyną podstawą prawną, która mogłaby takie profilowanie zalegalizować, może być szczególny przepis prawa.

Jeżeli zgoda na profilowanie została pobrana przy pomocy dedykowanej strony internetowej, odwołanie zgody musi być możliwe w ten sam sposób.

Odwołanie zgody wywołuje wyłącznie skutki na przyszłość - oznacza to, że od chwili otrzymania oświadczenia o odwołaniu zgody, nie można już opierać na zgodzie przetwarzania danych.

3. Realizacja prawa do sprzeciwu

Administrator, po wniesieniu sprzeciwu przez osobę, której dane przetwarzał, powinien zaprzestać przetwarzania tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Nawet jeżeli dane osobowe mogą być przetwarzane zgodnie z prawem, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi lub ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej, każdej osobie, której dane dotyczą, przysługuje prawo sprzeciwu wobec przetwarzania danych osobowych dotyczących jej szczególnej sytuacji.

Wykazanie zaistnienia ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń, jest obowiązkiem leżącym po stronie Administratora, i ma on obowiązek wykazania powyższego, w ewentualnym postępowaniu przed organem nadzorczym.

Wykorzystanie prawa do sprzeciwu nie prowadzi do automatycznego usunięcia wszystkich danych osobowych przez Administratora. Oznacza ono, że Administrator, z chwilą otrzymania sprzeciwu wobec przetwarzania danych osobowych, zaprzestaje z nich korzystać.

Aby dane osobowe zostały całkowicie usunięte konieczne jest skorzystanie przez osobę, której dane przetwarza Administrator, z prawa do usunięcia danych osobowych - prawa do bycia zapomnianym.

Zasady powoływania i funkcjonowania inspektora ochrony danych osobowych

1. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań przewidzianych w przepisach prawa.
2. W przypadku powierzenia funkcji inspektora ochrony danych osobie dotychczas zatrudnionej w organie, zawierana jest z nim dodatkowa umowa o świadczenie usług.
3. W przypadku powierzenia funkcji inspektora ochrony danych osobie dotychczas niezatrudnionej w organie, zawierana jest z nim umowa o pracę lub umowa o świadczenie usług.
4. Inspektor ochrony danych bezpośrednio podlega bezpośrednio kierownikowi/dyrektorowi organu.
5. W związku z wykonywanymi zadaniami z zakresu ochrony danych osobowych, inspektor ochrony danych osobowych nie może być odwoływany ani karany.
6. Do zadań inspektora ochrony danych należy w szczególności:

   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

   b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

   d) współpraca z organem nadzorczym;

   e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Standardy zabezpieczeń stosowane w jednostce

Środki techniczne i organizacyjne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:

a) wszystkie pomieszczenia, w których przetwarzane są dane osobowe w przypadku ich opuszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych zamykane są na klucz (także w godzinach pracy),
b) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej płyty CD, DVD, dyskietki) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe w szafach pancernych lub metalowych,
c) nieaktualne lub błędne wydruki zawierające dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę placówki,
d) wynoszenie akt i dokumentów, zawierających dane osobowe (np. dzienniki lekcyjne, dzienniki zajęć) poza teren placówki jest kategorycznie zabronione,
e) budynek, w którym są przetwarzane dane chroniony jest całodobowo przez pracowników ochrony.

2. Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:

a) zbiory danych osobowych przetwarzane są przy użyciu komputerów stacjonarnych i przenośnych,
b) udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe przez administratora sieci następuje na podstawie upoważnienia do przetwarzania danych osobowych,
c) każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych zobowiązany jest do zapoznania się oraz stosowania przepisów ustawy ochronie danych osobowych i instrukcji wewnętrznych,
d) osobom upoważnionym do przetwarzania danych osobowych przydziela się indywidualne identyfikatory, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania,
e) do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń ASI,
f) operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać osoba upoważniona po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek,
g) monitory na stanowiskach pracy ustawione są w sposób uniemożliwiający wgląd w dane osobowe,
h) na komputerach instaluje się systemowe mechanizmy wymuszające okresową zmianę haseł,
i) pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej,
j) przed atakami z sieci zewnętrznej wszystkie komputery administratora danych chronione są środkami dobranymi przez administratora systemów informatycznych ASI. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora systemów informatycznych ASI oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa,
k) stosowanie urządzeń UPS, chroniący system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
l) udostępnianie kluczy do pomieszczeń, w których przetwarzane są dane osobowe jest tylko osobom upoważnionym.

5. Organizację ochrony danych osobowych realizuje się poprzez:

a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do

pracy,

b) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych i programów,
c) kontrolowanie pomieszczeń budynku,
d) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
e) zabezpieczenie obiektu.

Rejestr operacji przetwarzania danych osobowych oraz Rejestr czynności przetwarzania danych osobowych

2. Rejestr operacji przetwarzania danych osobowych .

Dane kontaktowe		
	Dane	Uwagi
Imię i nazwisko / nazwa administratora danych	Dyrektor Mgr Marta Dibelka	
Kontakt do administratora danych	41 367-76-167	
Kontakt do współadministratora danych		
Imię i nazwisko / nazwa przedstawiciela administratora danych		
Kontakt do przedstawiciela administratora danych		
Imię i nazwisko / nazwa inspektora ochrony danych	Aleksandra Bartosz	
Kontakt do inspektora ochrony danych	email: iod@sp31.kielce.eu ; tel: 41 36 76 250	
Cele przetwarzania danych osobowych		
	Opis celów	Uwagi
Wynikające z ustawy Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe – t.j. Dz.U. 2018 poz. 996, 1000 i 1290; Ustawa z dnia 7 września 1991 r. o systemie oświaty – t.j. Dz.U. 2017 poz. 2198; Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej - Dz.U. 2017 poz. 2159 ze zm. o systemie oświaty	Dopełnienie obowiązków określonych przepisami , m.in.: -rekrutacja do oddziałów przedszkolnych, klas I - przyjęcia dziecka do szkoły, - realizacja zadań oświatowych, - realizacja orzeczeń wydanych, m.in. przez MZPPP w Kielcach, - zapewnienie bezpieczeństwa dziecka w czasie pobytu w szkole, - umożliwienie dziecku korzystania z pełnej oferty szkoły, - realizacja działań promocyjnych szkoły, - prowadzenie ewidencji uczniów i wychowanków, - prowadzenie ewidencji dzieci zamieszkałych w obwodzie szkoły; - prowadzenie ewidencji uczniów korzystających ze świetlicy i żywienia; - prowadzenie ewidencji osób upoważnionych do odbioru dziecka ze świetlicy i oddziału przedszkolnego, - organizacja konkursów międzyszkolnych, - inne wynikające z przepisów.	
Wynikające z Kodeksu Pracy USTAWA z dnia 26 czerwca 1974r. Kodeks pracy, Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej - Dz.U. 2017 poz. 2159 ze zm.	Uprawnienia, obowiązki wynikające z zatrudnienia, m.in.: - rekrutacja na wolne stanowiska, - zatrudnianie, zwalnianie pracowników, - wypłata wynagrodzenia lub innych świadczeń, - plany urlopowe, ewidencja czasu pracy, - harmonogramy dozorców i innych pracowników, - listy obecności pracowników administracji i obsługi, - staże.	
Wynikające z Kodeksu cywilnego Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. 2018 poz.1025)	Dopełnienie obowiązków określonych przepisami , m.in.: - realizacja umów cywilno - prawnych zawartych z osobami spoza jednostki, - roszczenie należności, np. z tytułu najmu pomieszczeń szkoły, - udzielanie pełnomocnictwa.	

Wynikające z USTAWA z dnia 26 stycznia 1982 r. Karta Nauczyciela.	Dopełnienie obowiązków określonych przepisami , m.in.: - zatrudniania nauczycieli, ich prawa i obowiązki	
Wynikające z Ustawy z dnia 14 czerwca 1960r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2017 poz. 1257)	Dopełnienie obowiązków określonych przepisami , m.in.: - rozpatrywanie skarg i wniosków, - prowadzenie rejestru korespondencji	
Wynikające z ustawy o pomocy państwa w wychowywaniu dzieci	Dopełnienie obowiązków określonych przepisami , m.in.: - zgłaszanie dzieci do MOPR, MOPS, MGOPS - zgłaszanie do udzielania stypendium socjalnego	
Wynikające z ustawy o przeciwdziałaniu przemocy w rodzinie	Dopełnienie obowiązków określonych przepisami , m.in.: - zgłaszanie incydentów do odpowiednich służb - wypełnienie niebieskiej karty	
Wynikające z Ustawy z dnia 21 listopada 2008 r. w sprawie zatrudniania pracowników samorządowych.	Dopełnienie obowiązków określonych przepisami, m.in.: - wysokości wypłat	
Wynikające z Ustawy z dnia 4 marca 1994r. o zakładowym funduszu świadczeń socjalnych (t.j. Dz. U. z 2018 poz. 1316)	Dopełnienie obowiązków określonych przepisami , m.in.: - zbieranie i przekazywanie informacji o emerytach do Zespołu Obsługi Socjalnej Emerytów i Rencistów	
Wynikające z Ustawy z dnia 14 lipca 1983r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz. U. z 2018 poz. 217)	Dopełnienie obowiązków określonych przepisami , m.in.: - gromadzenie i przechowywanie dokumentacji szkoły.	
Wynikające z Ustawy z dnia 6 września 2001r. o dostępie do informacji publicznej (t.j. z 2018 poz. 1330)	Dopełnienie obowiązków określonych przepisami , m.in.: - udzielanie informacji osobom ubiegającym się o uzyskanie informacji publicznej.	

<u>Przetwarzane dane osobowe</u>

	Opis kategorii danych	Przewidywany termin usunięcia danych
Kategorie przetwarzanych danych osobowych dzieci / rodziców/ opiekunów prawnych/ nauczycieli / pracowników administracji i obsługi / innych pracowników	imię i nazwisko dziecka/ rodziców/prawnych opiekunów adres zamieszkania dziecka /rodziców/prawnych opiekunów PESEL data i miejsce urodzenia dziecka numer legitymacji szkolnej płeć numer telefonu/rodziców/prawnych opiekunów adresy poczty elektronicznej/rodziców/prawnych opiekunów wizerunek dziecka , rodzica/ prawnego opiekuna (w przypadku imprez szkolnych / publicznych) numer i seria dowodu osobistego/rodziców/prawnych opiekunów	50 lat
nauczycieli / pracowników administracji i obsługi obecnych i byłych/ innych pracowników/ emerytów	imię i nazwisko, nazwisko rodowe matki, adres zamieszkania PESEL, NIP data i miejsce urodzenia dziecka płeć numer telefonu adresy poczty elektronicznej wizerunek numer i seria dowodu osobistego	50 lat

	wykształcenie zawód stopień awansu zawodowego w przypadku nauczycieli imiona i daty urodzenia współmałżonka i dzieci nr rachunku bankowego pracowników	
studenci/stażyści	imię i nazwisko, nazwisko rodowe matki adres zamieszkania PESEL data i miejsce urodzenia dziecka płeć numer telefonu adresy poczty elektronicznej wizerunek numer i seria dowodu osobistego wykształcenie zawód	5 lat
Osoby objęte monitoringiem	Wizerunek osób objętych monitoringiem wizyjnym	3 miesiące
Szczególne kategorie przetwarzanych danych osobowych	• stan zdrowia dziecka (orzeczenia lekarskie) • pochodzenie • wyznanie religijne	
	Opis kategorii osób	Uwagi
Kategorie osób, których dane dotyczą	Uczniowie, Nauczyciele Pracownicy administracji Pracownicy obsługi Rodzice / opiekunowie prawni	
Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	Pielęgniarka - Badania okresowe dzieci Informatyk BHP Lekarz medycyny pracy GOPS	– dane przekazywane do dalszego prowadzenia procesu nauczania i wychowania,

3. Rejestr czynności przetwarzania danych osobowych (załącznik w pliku Ms Excel .xlsx)

Polityka monitorowania i reagowania na naruszenia ochrony danych

Polityka monitorowania ochrony danych

1. Bieżący monitoring przestrzegania niniejszej polityki, stosowania przewidzianych nią procedur oraz adekwatności stosowanych środków zabezpieczeń dokonywany jest przez inspektora ochrony danych.

2. Inspektor ochrony danych przynajmniej raz na 6 miesięcy dokonuje audytu polityki bezpieczeństwa w zakresie stosowania przewidzianych nią procedur oraz adekwatności stosowanych środków zabezpieczeń. Po przeprowadzonym audycie inspektor zobowiązany jest opracować pisemny raport dla administratora danych. Raport powinien zawierać ocenę oraz propozycje w zakresie ewentualnych modyfikacji stosowanych procedur oraz środków zabezpieczeń.

3. Na podstawie raportu wskazanego w pkt 2. administrator danych określa kierunki ewentualnych zmian oraz określa termin na ich wprowadzenie.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych

d) 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.

Rejestr incydentów.

I.	Data zdarzenia	
1.	imię i nazwisko osoby zgłaszającej incydent	
2.	imię i nazwisko osoby przyjmującej zgłoszenie incydentu	
3.	data i godzinę przyjęcia zgłoszenia incydentu	
4.	określenie czasu i miejsca incydentu	
5.	opis zgłoszonego incydentu oraz okoliczności towarzyszące	
6.	przyczyny wystąpienia naruszenia	
7.	opis podjętych działań naprawczych	
8.	wyniki przeprowadzonego badania wyjaśniającego	
9.	ocena skuteczności przeprowadzonego postępowania naprawczego	
10.	podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości naruszenia ochrony danych osobowych	

Wykaz pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe

Lp.	Nazwa pomieszczenia	Lokalizacja	Rodzaj Zabezpieczenia	Typ danych w pomieszczeniu
Budynek piętrowy usytuowany nr 31 z Oddziałami Integracyjnymi im Henryka Sienkiewicza w Kielcach, ul. Partyzantów 17 Bieliny, z parkingiem przed budynkiem dla pracowników/gości, teren ogrodzony, zamykany na klucz, wyposażony w monitoring dla zachowania bezpieczeństwa.				
1.	Sekretariat	Poziom parteru	1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenia zamykane na klucz, 3. Wszystkie klucze zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane szczególnie chronione dane dostępne i przetwarzane na bieżąco.
2.	Gabinet Dyrektora / Wicedyrektorów	Poziom parteru	1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane szczególnie chronione. Dane dostępne i przetwarzane na bieżąco. Dane przechowywane w systemie zarządzania Szkołą oraz w wersji papierowej –
3.	Sale lekcyjne	Poziom Parter 1 Piętro	1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane szczególnie chronione. Dane dostępne i przetwarzane na bieżąco tylko podczas zajęć lekcyjnych
4.	Pokój pielęgniarki szkolnej / gabinet zabiegowy	Poziom	1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym. 5.	Dane zwykłe, dane szczególnie chronione dane dostępne i przetwarzane na bieżąco.
5.	Pokój nauczycielski	Poziom Piętro 1	1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z	Dane zwykłe, dane szczególnie chronione dane dostępne i przetwarzane na bieżąco.

			kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	
6.	Pokój pedagoga szkolnego/ logopedy	Poziom	1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane szczególnie chronione dane dostępne i przetwarzane na bieżąco.
7.	Archiwum szkolne	Poziom	1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane szczególnie chronione dane dostępne i przetwarzane na bieżąco.

Procedura wyboru i weryfikacji podmiotu przetwarzającego dane.

1) Każdy podmiot zewnętrzny przetwarzający dane zgromadzone przez tut. organ ma obowiązek zapewnić adekwatne środki i standardy zabezpieczenia przekazanych mu danych.
2) Warunkiem przekazania podmiotowi zewnętrznemu danych zgromadzonych przez tut. organ jest zawarcie z podmiotem zewnętrznym umowy o powierzenie danych osobowych
3) Wzór umowy o powierzenie danych osobowych znajduje się w wykazie dokumentów załączonych do niniejszej polityki.

6. Wykaz podmiotów przetwarzających dane na zlecenie administratora danych.

Lp.	**Nazwisko i Imię / Firma**	**Rodzaj powiązania / umowy z administratorem**	**Rodzaj Uprawnienia / Cel przetwarzania**	**Typ powierzonych danych.**	**Okres powierzenia**	**Zastosowane środki bezpieczeństwa ochrony danych osobowych**
1.		Umowa o wykonywaniu usług –	Umowa powierzenia danych	Uprawnienie do danych zwykłych i szczególnie chronionych	Czas trwania umowy	Dane przesyłane przez upoważnione osoby – bezpośrednio do placówki przetwarzającej i ADO.
2.		Umowa o wykonywaniu usług związanych z dostawą i serwisem systemu zarządzania placówką	Umowa powierzenia danych	Uprawnienie do danych zwykłych i szczególnie chronionych	Czas trwania umowy	Dane przesyłane przez upoważnione osoby – bezpośrednio do placówki przetwarzającej i ADO. Pełne zabezpieczenia systemów informatycznych.
3.						

Administrator Danych Osobowych

.....
Podpis