POLITYKA BEZPIECZEŃSTWA OCHRONY I PRZETWARZANIA DANYCH OSOBOWYCH WRAZ Z INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Publiczna Szkoła Podstawowa im. św. Jadwigi Królowej w Bilczy

Bilcza 2019

Spis treści

1 Wstęp.

1.1 Informacje ogólne.

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Publiczną Szkołę Podstawową im. św. Jadwigi Królowej w Bilczy (dalej jako „Szkoła Podstawowa") przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Wprowadzenie Polityki zmierza do zapewniania zgodności działania administratora danych z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) stosowanym od dnia 25 maja 2018 r., ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych wchodzącą w życie dnia 25 maja 2018 r. oraz ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. - Dz. U. z 2016 r., poz. 922 z późn. zm.) w zakresie w jakim nie traci mocy w dniu 25 maja 2018 r. tj. art. 1, art. 2, art. 3 ust. 1, art. 4-7, art. 14-22, art. 23-28, art. 31 oraz rozdziałów 4, 5 i 7, które zachowują moc w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie, w terminie do dnia wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89).

Wskazane dane osobowe będą przetwarzane przez Szkołę Podstawową wyłącznie w celach określonych w niniejszym dokumencie.

Polityka obowiązuje wszystkich pracowników Szkoły Podstawowej oraz podmioty współpracujące lub świadczące na jego rzecz usługi na podstawie umów cywilnoprawnych, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Przetwarzanie danych osobowych w Szkole Podstawowej odbywa się w wersji papierowej i za pomocą systemów informatycznych.

Administratorem danych osobowych przetwarzanych w ww. sposób jest Szkoła Podstawowa.

Polityka Bezpieczeństwa została opracowana w oparciu o wytyczne i zalecenia zawarte w przepisach:

1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) stosowanym od dnia 25 maja 2018 r.;
2) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych wchodzącą w życie dnia 25 maja 2018 r.;

3) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. - Dz. U. z 2016 r., poz. 922 z późn. zm.) w zakresie w jakim nie traci mocy w dniu 25 maja 2018 r. tj. art. 1, art. 2, art. 3 ust. 1, art. 4-7, art. 14-22, art. 23-28, art. 31 oraz rozdziałów 4, 5 i 7, które zachowują moc w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie, w terminie do dnia wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89),
4) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100 poz. 1024 z późn zm.),
5) rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. 2015 r., poz. 719 z późn. zm.),
6) rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. 2015 r., poz. 745 z późn. zm.).

Polityka Bezpieczeństwa uwzględnia również wytyczne i zalecenia zawarte w przepisach unijnych o ochronie danych osobowych dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

1.2 Zakres informacji objętych Polityką Bezpieczeństwa oraz zakres zastosowania.

Niniejsza Polityka Bezpieczeństwa określa zasady i procedury związane z przetwarzaniem danych osobowych. Jednocześnie wskazany dokument zawiera opis sposobów zabezpieczenia przetwarzanych danych osobowych.

Polityka Bezpieczeństwa zawiera informacje na temat:

1) wykazu i zakresu przetwarzanych danych osobowych;
2) programów stosowanych do przetwarzania ww. danych;
3) wykazu budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe;
4) opisu struktury zbiorów danych z uwzględnieniem zawartości poszczególnych pól informacyjnych i istniejących pomiędzy nimi powiązań;
5) sposobu przepływu danych pomiędzy poszczególnymi systemami,
6) środków technicznych i organizacyjnych wykorzystywanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych;
7) sposobu zarządzania systemem informatycznym zawierającym dane osobowe;
8) procedur postępowania w przypadku naruszenia postanowień i zasad Polityki Bezpieczeństwa.

1.3 Wyjaśnienie terminów używanych w dokumencie Polityki Bezpieczeństwa.

1) **Administrator Danych Osobowych – Publiczna Szkoła Podstawowa im. św. Jadwigi Królowej w Bilczy ,** Bilcza 75, 27-641 Obrazów, Numer RSPO: 14231
2) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której dane są przetwarzane Szkołę Podstawową**,**
3) **Uczeń-** należy przez to rozumieć osobę, która realizuje obowiązek szkolny w ramach bądź obowiązek nauki w ramach jednostki administracyjnej jaką jest Administrator Danych Osobowych.
4) **Identyfikator** – należy przez to rozumieć elektroniczne, indywidualne oznaczenie pracowników w systemie informatycznym tzw. login,
5) **Pracownik —** należy przez to rozumieć osobę zatrudnioną przez Szkołę Podstawową w formie umowy o pracę lub świadcząca na jego rzecz usługi na podstawie umów cywilno – prawnych.
6) **Użytkownik systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Szkoły Podstawowej, Użytkownikiem systemu może być Pracownik.
7) **Ustawa** – należy przez to rozumieć ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych wchodzącą w życie dnia 25 maja 2018 r.
8) **Dawną ustawa -** należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r., poz. 1182 z późn. zm.).
9) **Rozporządzenie** lub **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) stosowanym od dnia 25 maja 2018 r.;

10) **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.
11) **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

2 Osoby odpowiedzialne za ochronę danych osobowych.

2.1 Informacje ogólne.

Do kręgu osób odpowiedzialnych za przetwarzanie i ochronę danych osobowych Szkole Podstawowej należy zaliczyć:

1) Administratora Danych Osobowych,
2) Inspektora Ochrony Danych (tylko i wyłącznie w przypadku powołania - Załącznik nr 5 do Polityki Bezpieczeństwa),
3) Administrator Systemów Informatycznych (tylko i wyłącznie w przypadku powołania - Załącznik nr 7 do Polityki Bezpieczeństwa),
4) osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Szkoły Podstawowej , które uzyskały pisemne upoważnienie do przetwarzania danych osobowych.

Wskazane podmioty mają stały i regularny dostęp do danych osobowych, przetwarzając je oraz uniemożliwiając dostęp do nich osobom nieuprawnionym.

2.2 Administrator Danych Osobowych.

Administratorem Danych Osobowych jest **Publiczna Szkoła Podstawowa im. św. Jadwigi Królowej w Bilczy,** Bilcza 75, 27-641 Obrazów, Numer RSPO: 14231 Administrator Danych Osobowych decyduje o celach i środkach przetwarzania danych osobowych.

Do obowiązków Administratora Danych Osobowych należą:

1) stosowanie środków technicznych i organizacyjnych zapewniających przetwarzanym danym odpowiednią ochronę,
2) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zebraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem,
3) dopełnienie obowiązku informacyjnego, tj.:
   a) w przypadku zbierania danych bezpośrednio od osoby, której dotyczą informowanie jej o swojej nazwie i adresie, celu zbierania, odbiorcach danych (także tych przewidywanych), prawie dostępu do danych i prawie ich poprawiania, a także o dobrowolności albo obowiązku ich podania,
   b) w przypadku zbierania danych nie od osoby, której one dotyczą informowanie osoby, której one dotyczą, o swojej nazwie i adresie, celu i zakresie zbierania danych, a zwłaszcza o ich odbiorcach, źródle, z którego dane pozyskał, prawie dostępu do danych i prawie ich poprawiania, a także o prawie żądania zaprzestania przetwarzania danych lub wniesienia sprzeciwu wobec przetwarzania danych,
4) dokładanie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, poprzez zapewnienie, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów,

w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,

5) respektowanie prawa osób, których przetwarzane dane dotyczą,
6) nadawanie i odwoływanie upoważnienia do przetwarzania danych osobowych Inspektorowi Ochrony Danych,
7) powierzanie podmiotom trzecim przetwarzania danych osobowych na podstawie pisemnych umów.

Administrator Danych Osobowych wypełnia również obowiązki i uprawnienia opisane w pkt. 2.3 Polityki Bezpieczeństwa w przypadku, gdy nie ustanowi lub nie ma obowiązku ustanowienia Inspektora Ochrony Danych.

2.3 Inspektor Ochrony Danych.

Wyznaczenie Inspektora Ochrony Danych jest obowiązkiem, w przypadku gdy Administrator Danych Osobowych przetwarza dane, w sytuacjach o których mowa w art. 37 ust. 1 Rozporządzenia tj.:

a) administratorem danych jest organ lub podmiot publiczny;
b) główna działalność administratora polega na operacjach przetwarzania wymagających regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
c) główna działalność administratora polega na przetwarzaniu na dużą skalę wrażliwych danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

W każdym innym przypadku wyznaczenie Inspektora Ochrony Danych jest prawem, ale nie obowiązkiem Administratora Danych Osobowych.

Decyzja o jego wyznaczeniu należy do Administratora Danych Osobowych, co zostaje potwierdzone stosownym dokumentem (Załącznik nr 5 do Polityki Bezpieczeństwa).

Do uprawnień i obowiązków Inspektora Danych Osobowych należą:

1) stały nadzór nad treścią Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym,
2) aktualizacja i modyfikacja ww. dokumentów,
3) czynności sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania,
4) informowanie Administratora Danych Osobowych oraz Pracowników o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz przepisów Ustawy lub Dawnej Ustawy;
5) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania
6) prowadzenie jawnego rejestru zbiorów danych osobowych,
7) udział w kontrolach prowadzonych przez kontrolerów organu nadzorczego i współpraca z organem nadzorczym;
8) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych

z przetwarzaniem i konsultacjami w zakresie przetwarzania danych osobowych.

9) udzielanie odpowiedzi na zapytania kierowane do Administratora Danych Osobowych przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,

10) nadawanie i odbieranie poszczególnym Pracownikom upoważnień do przetwarzania danych osobowych oraz przeprowadzanie dla nich szkoleń z zakresu ochrony danych osobowych (na podstawie upoważnienia stanowiącego Załącznik nr 6 do Polityki Bezpieczeństwa),

11) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,

12) prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych,

13) nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe,

14) monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.

Inspektor Ochrony Danych wypełnia również obowiązki i uprawnienia opisane w pkt. 2.4. Polityki Bezpieczeństwa w przypadku, gdy Administrator Ochrony Danych Osobowych nie ustanowi Administratora Systemów Informatycznych.

2.4 Administrator Systemów Informatycznych.

Wyznaczenie Administratora Systemów Informatycznych nie jest obowiązkiem, ale prawem Administratora Danych Osobowych. Decyzja o jego wyznaczeniu należy do Administratora Danych Osobowych, co zostaje potwierdzone stosownym dokumentem (Załącznik nr 7 do Polityki Bezpieczeństwa).

Do uprawnień i obowiązków Administratora Systemów Informatycznych należą:

1) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,

2) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,

3) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,

4) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych.

W przypadku nieustanowienia Administratora Systemów Informatycznych przez Administratora Danych Osobowych, jego obowiązki i uprawnienia przejmuje Inspektor Ochrony Danych, a w przypadku jego braku Administrator Danych Osobowych.

2.5 Osoby upoważnione do przetwarzania danych osobowych – Użytkownicy systemu.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych.

Osoba, która uzyskała upoważnienie do przetwarzania danych osobowych tj. Użytkownik systemu zobowiązana jest do ich ochrony w sposób zgodny z przepisami Rozporządzenia, Ustawy, Dawnej Ustawy, rozporządzeń wymienionych w pkt. 1.1. niniejszego dokumentu, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.

Jednym z obowiązków Użytkownika systemu jest obowiązek zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten trwa również po ustaniu zatrudnienia wskazanej osoby.

Upoważnienie udzielane jest w formie pisemnej, przez Administratora Danych Osobowych lub – w przypadku, gdy został powołany – Inspektor Ochrony Danych. Upoważnienie sporządzane jest wg wzorów stanowiących Załączniki nr 8a i 8b do niniejszej Polityki. Treść upoważnienia różni się w zależności, czy osobą upoważnioną jest Pracownik, czy osoba związana z Administratorem Danych Osobowych innym stosunkiem zobowiązaniowym.

2.6 Rejestr Użytkowników systemu.

Administrator Danych Osobowych jest zobowiązany do prowadzenia rejestru Użytkowników systemu i ich uprawnień w systemie informatycznym.

Rejestr musi odzwierciedlać aktualny stan systemu w zakresie Użytkowników systemu oraz umożliwić przeglądanie historii zmian w systemie informatycznym.

Rejestr zawiera następujące dane:

1) imię i nazwisko Użytkownika systemu,

2) datę nadania uprawnień,

3) datę odebrania uprawnień,

4) przyczynę odebrania uprawnień,

5) nazwy zbiorów objętych zakresem upoważnienia.

Rejestr Użytkowników Systemu prowadzony jest w wersji papierowej, jak również elektronicznej. Po każdej zmianie jego treści tworzona jest nowa wersja papierowa i elektroniczna wskazanego rejestru, a stara jest archiwizowana.

2.7 Odpowiedzialność Użytkowników systemu.

Użytkownik systemu ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

Użytkownik systemu ponosi wszelką odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu z wyjątkiem sytuacji, kiedy Administrator Danych Osobowych lub Inspektor Ochrony Danych użyje hasła Użytkownika podczas jego nieobecności. Administrator Danych Osobowych lub Inspektor Ochrony Danych ma obowiązek sporządzić z tego zdarzenia protokół, z którym zostaje zapoznany Użytkownik systemu, którego hasło zostało użyte. Po zapoznaniu się z protokołem, Użytkownik systemu ma obowiązek dokonać natychmiastowej zmiany hasła dostępu i przekazać je

Administratorowi Danych Osobowych lub Inspektorowi Ochrony Danych w zamkniętej i podpisanej kopercie.

Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przyznanych uprawnień, traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

W uzasadnionych sytuacjach Administrator Danych Osobowych lub Inspektor Ochrony Danych może odebrać uprawnienia Użytkownikowi systemu z podaniem daty oraz przyczyny odebrania uprawnień. W takiej sytuacji należy sporządzić notatkę służbową.

Hasło oraz uprawnienia Użytkownika systemu, który je utracił, należy niezwłocznie wyrejestrować z systemu informatycznego. Wyrejestrowania z systemu dokonuje Administrator Danych Osobowych lub Inspektor Ochrony Danych.

Użytkownik systemu zobowiązany jest do zachowania ich w poufności oraz dołożenia wszelkich starań, aby dane osobowe nie zostały przekazane osobom nieuprawnionym.

3 Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych.

Administrator Danych Osobowych lub Inspektor Ochrony Danych, może przekazywać Użytkownikom systemu będącymi Pracownikami lub podmiotom współpracującym z Szkołą Podstawową na podstawie umów cywilnoprawnych przetwarzanie danych osobowych. Przekazanie przetwarzania danych osobowych w zależności od stosunku łączącego Szkołę Podstawową z danym Użytkownikiem systemu może nastąpić na podstawie upoważnienia lub umowy o przetwarzanie danych osobowych.

3.1 Upoważnienie do przetwarzania danych osobowych.

Upoważnienie do przetwarzania danych osobowych, którego wzory stanowią Załączniki nr 8a i 8b do Polityki Bezpieczeństwa jest dokumentem dającym określonym osobom prawo do przetwarzania ściśle określonych danych osobowych.

Upoważnienia do przetwarzania danych osobowych są nadawane przez Administratora Danych Osobowych lub – jeżeli został wyznaczony – Inspektora Ochrony Danych. Upoważnienie do przetwarzania danych osobowych Inspektorowi Ochrony Danych może być nadane wyłącznie przez Administratora Danych Osobowych. Inspektor Ochrony Danych nadaje Użytkownikom systemu upoważnienia do przetwarzania danych osobowych na podstawie stosownego upoważnienia nadanego mu przez administratora Danych Osobowych (wzór w Załączniku nr 6 do Polityki Bezpieczeństwa).

Upoważnienie nadawane jest przez Administratora Danych Osobowych lub Inspektora Ochrony Danych z urzędu lub na wniosek bezpośredniego przełożonego Pracownika, samego Pracownika lub innego Użytkownika systemu.

Upoważnienie nadawane jest wyłącznie w formie pisemnej.

O nadawaniu ww. upoważnień decyduje Administrator Danych Osobowych lub Inspektor Ochrony Danych. W takim samym zakresie wskazane podmioty ponoszą odpowiedzialność za nadawanie ww. uprawnień.

W upoważnieniu dokładnie określony jest zbiór danych osobowych, które Użytkownik systemu będzie mógł przetwarzać, jak również cel wskazanego przetwarzania.

Po nadaniu upoważnienia dane Użytkownika systemu wprowadzane są przez Administratora Danych Osobowych lub Inspektora Ochrony Danych do specjalnie w tym celu prowadzonego rejestru Użytkowników Systemu (pkt. 2.6. Polityki Bezpieczeństwa).

Rejestr Użytkowników Systemu prowadzony jest w wersji papierowej, jak również elektronicznej. Po każdej zmianie jego treści tworzona jest nowa wersja papierowa i elektroniczna wskazanego rejestru, a stara jest archiwizowana.

3.2 Umowy powierzenia przetwarzania danych osobowych.

Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych podmiotom trzecim na podstawie pisemnej umowy. Wskazane uprawnienie nie może być wykonywane przez Inspektora Ochrony Danych.

Umowa, na podstawie której nastąpi przekazanie przetwarzania danych osobowych nie musi dotyczyć wyłącznie kwestii dotyczącej przetwarzania danych osobowych. Przedmiot wskazanej umowy może być zatem różny. Istotne jest jednakże, aby umowa

zawierała konkretne zapisy dotyczące powierzenia danemu podmiotowi przetwarzania danych osobowych. W umowie nie może również zabraknąć określenia celu w jakim będą przetwarzane dane osobowe – najczęściej będzie to cel związany z wykonaniem przedmiotu umowy.

Ww. umowa musi być zawarta w formie pisemnej.

Wykaz podmiotów, którym Administrator Danych Osobowych powierzył przetwarzane danych osobowych na podstawie pisemnej umowy stanowi Załącznik nr 11 do Polityki Bezpieczeństwa.

4 Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych.

Podmiotem odpowiedzialnym za przetwarzanie danych osobowych i ich bezpieczeństwo jest Administrator Danych Osobowych.

Zważywszy jednakże na wielość osób uprawnionych do przetwarzania danych osobowych i związane z tym ryzyko niebezpieczeństwa udostępnienia danych osobowych podmiotom nieupoważnionym ustala się następujące ogólne zasady bezpieczeństwa przy przetwarzaniu danych osobowych:

1) za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną i bezpośrednią odpowiedzialność każdy Użytkownik systemu mający dostęp do wskazanych danych osobowych,
2) Użytkownik systemu nie może ujawnić przetwarzanych danych osobowych, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych,
3) zakaz ujawniania przetwarzanych danych osobowych obowiązuje w miejscu pracy, jak i poza nim, jak również po ustaniu stosunku pracy lub stosunku zobowiązaniowego,
4) Użytkownik systemu zobowiązany jest do zachowania porządku i czystości w swoim miejscu pracy lub innym miejscu, w którym przetwarza dane osobowe porządku. Obowiązuje go bezwzględny zakaz pozostawiania materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym („*zasada czystego biurka*"),
5) Użytkownik systemu zobowiązany jest niszczyć brudnopisy, błędne lub zbędne kopie materiałów zawierające dane osobowe w sposób uniemożliwiający odczytanie zawartej w nich treści, z wykorzystaniem przeznaczonych do tego urządzeń biurowych (niszczarki),
6) obowiązuje bezwzględnych zakaz wynoszenie jakichkolwiek materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych,
7) osoby nieupoważnione do przetwarzania danych osobowych mogą przebywać w pomieszczeniach, w którym przetwarzane są dane osobowe tylko w obecności osoby Użytkownika systemu, Administratora Danych Osobowych, Inspektora Ochrony Danych lub Administratora Systemów Informatycznych, chyba że dane te są zabezpieczone przed dostępem osób trzecich,
8) Użytkownicy systemu zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe, w czasie ich nieobecności w danym pomieszczeniu i nie pozostawiania kluczy w zamkach drzwi,
9) Użytkownicy systemu zobowiązani są do zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem,
10) Użytkownicy systemu zobowiązani są wylogować się lub wyłączać komputery, w których przetwarzane są dane osobowe, w każdym przypadku odejścia od wskazanego sprzętu.

5 Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.

W przypadku zaistnienia sytuacji, w której doszło do naruszenia ochrony danych osobowych, odpowiedzialność ponosi Administrator Danych Osobowych. Na nim ciąży obowiązek należytego wykonania wskazanych procedur zabezpieczających.

Administrator Danych Osobowych nie jest zobowiązany do wykonania ww. procedur jeżeli został powołany Inspektor Ochrony Danych, na którego przechodzi wskazana odpowiedzialność.

Jeżeli natomiast został ustanowiony Administrator Systemów Informatycznych odpowiedzialność za wdrożenie ww. postępowania ponosi wskazany podmiot.

Mając na uwadze powyższe w przypadku naruszenia ochrony danych osobowych obowiązują następujące procedury:

1) każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym Administratora Danych Osobowych, Inspektora Ochrony Danych lub Administratora Systemów Informatycznych,
2) Administrator Danych Osobowych (odpowiednio Inspektor Ochrony Danych lub Administratora Systemów Informatycznych) po otrzymaniu powiadomienia:
   d) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   e) sprawdza sposób działania programów (w tym obecność wirusów komputerowych),
   f) sprawdza jakość komunikacji w sieci telekomunikacyjnej,
   g) sprawdza zawartość zbioru danych osobowych,
   h) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,
3) w przypadku stwierdzenia naruszenia zabezpieczeń danych Administrator Danych Osobowych (odpowiednio Inspektor Ochrony Danych lub Administratora Systemów Informatycznych):
   a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.),
   b) w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej podejmuje odpowiednie kroki poprzez:
      - fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej,
      - wylogowanie Użytkownika systemu podejrzewanego o naruszenie zabezpieczenia ochrony danych,
      - zmianę hasła na konto Użytkownika systemu, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
   c) zabezpiecza i utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
   d) niezwłocznie przywraca prawidłowy stan działania systemu,

e) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,

f) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia,

4) jeżeli ww. raport sporządza Inspektor Ochrony Danych lub Administrator Systemów Informatycznych przekazuje on jego treść wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) Administratorowi Danych Osobowych,

5) Administrator Danych Osobowych (odpowiednio Inspektor Ochrony Danych lub Administratora Systemów Informatycznych), podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

a) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,

b) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza się dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych,

6) Administrator Danych Osobowych zawiadamia nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych organ nadzorczy.

6 Kontrola przetwarzania i stanu zabezpieczenia danych osobowych.

Nadzór i kontrolę nad ochroną przetwarzanych danych osobowych sprawuje Administrator Danych Osobowych.

Jeżeli został ustanowiony Inspektor Ochrony Danych przejmuje on ww. obowiązki w zakresie ochrony i nadzoru wskazanych danych osobowych.

Jeżeli został ustanowiony Administrator Systemów Informatycznych sprawuje on nadzór i kontrolę w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.

Czynności kontrolne przeprowadzane są co 6 miesięcy.

Z czynności kontrolnych sporządzany jest protokół, którego wzór stanowi Załącznik nr 12 do niniejszej Polityki.

W protokole zamieszcza się dokładny opis zakresu kontroli i przeprowadzonych czynności.

Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji przechowywanej u Administratora Danych Osobowych (w przypadku ustanowienia u Inspektora Ochrony Danych, a w zakresie systemów informatycznych u Administratora Systemów Informatycznych).

7 Opis struktury zbiorów danych wraz z zawartością poszczególnych pól informacyjnych i istniejących pomiędzy nimi powiązań.

Dane osobowe przetwarzane są przez Szkołę Podstawową w wersji elektronicznej oraz papierowej.

Dotyczą one uczniów i opiekunów prawnych uczniów, pracowników szkoły oraz osób współpracujących ze szkołą na podstawie umów cywilnoprawnych.

Wskazane zestawienie danych i ich opis wraz z zawartością poszczególnych pól informacyjnych i istniejących pomiędzy nimi powiązań stanowi Załącznik nr 1 do Polityki Bezpieczeństwa.

8 Sposób przepływu danych osobowych pomiędzy systemami informatycznymi.

Sposób przepływu danych pomiędzy systemami informatycznymi zależy od rodzaju stosowanego oprogramowania oraz rodzajów danych.
Mając na uwadze treść wykazu przetwarzanych danych osobowych zawartą w Załączniku nr 1 do Polityki Bezpieczeństwa, należy również w odniesieniu do poszczególnych pozycji omówić sposób przepływu danych pomiędzy systemami informatycznymi.
Opis ww. zagadnienia został przedstawiony w Załączniku nr 2 do Polityki Bezpieczeństwa.

9 Obszar, w którym przetwarzane są dane osobowe.

Przetwarzanie danych osobowych odbywa się w biurze firmy.

Dane dotyczące sprawozdawczości finansowej oraz dokumentacja pracownicza przechowywane są siedzibie Szkoły.

Szczegółowy wykaz i opis obszarów, w którym są przetwarzane dane osobowe, których administratorem jest Szkoła Podstawowa zostały ujęte w Załączniku nr 3 do Polityki Bezpieczeństwa.

Odnoście ww. obszarów stosowane są następujące procedury postępowania i środki bezpieczeństwa.

Dostęp do stref bezpośrednio związanych z przetwarzaniem danych osobowych (komputery, szafy z aktami) mają jedynie upoważnieni Pracownicy, podmioty przetwarzające dane na podstawie stosownych umów zawartych ze Szkołą Podstawową (Załącznik nr 10 do Polityki Bezpieczeństwa) oraz Administrator Danych Osobowych, a w przypadku powołania także, Inspektor Ochrony Danych i Administrator Systemów Informatycznych.

Zabrania się przebywania osób postronnych w strefach bezpośrednio związanych z przetwarzaniem danych osobowych (komputery, szafy z aktami).

10 Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Szkoła Podstawowa stosuje zróżnicowany wachlarz środków technicznych i organizacyjnych mających zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.

Szczegółowe zestawienie wskazanych środków zawierają wykazy stanowiący Załączniki nr 4a i 4b do Polityki Bezpieczeństwa.

11 Obowiązek informacyjny w przedmiocie przetwarzania danych osobowych.

Szkolą Podstawowa wypełnia obowiązek informacyjny o zakresie, celu, miejscu i czasie przetwarzania znajdujących się w jego posiadaniu danych osobowych.

W ramach realizacji ww. obowiązku Szkoły Podtsawowej podaje osobom, których dane osobowe są przetwarzane, następujące informacje:

a) swoją tożsamość i dane kontaktowe;

b) dane kontaktowe Inspektora Ochrony Danych, jeżeli zostanie powołany;

c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

d) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;

e) informacje o ewentualnym zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi Rozporządzenia, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

f) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

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

h) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

i) informacje o prawie wniesienia skargi do organu nadzorczego;

j) informację, 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.

Wzór informacji dotyczącej danych przetwarzanych przez Szkołę Podstawową wraz z wykazem lokalizacji i sposobów ich udostępniania stanowi Załącznik nr 13 do Polityki Bezpieczeństwa.

12 Procedura związana ze sprostowaniem, ograniczeniem i usuwaniem danych osobowych oraz sprzeciwem.

Szkoła Podstawowa realizuje obowiązki związane ze sprostowaniem, ograniczeniem i usuwaniem danych osobowych.

Dokonanie ww. czynności następuje na wniosek podmiotu, którego dane osobowe dotyczą po zgłoszeniu i pozytywnej weryfikacji jego żądania.

Pozytywna weryfikacja żądania zgłoszonego przez osobę, której dane osobowe dotyczą odbywa się wg poniższych zasad:

1. Osoba żądająca sprostowania, ograniczenia i usunięcia danych osobowych lub składająca sprzeciw ma obowiązek wykazać, że jest uprawniona do wystosowania ww. żądania;
2. Kierowanie ww. żądań następuje w takiej formie w jakiej osoba, której dane są przetwarzane wyraziła zgodę, w każdym innym przypadku odbywa się to w formie pisemnej pod rygorem nieważności z podpisem potwierdzonym przez Szkołę Podstawową za okazaniem dowodu osobistego, lub notarialnie poświadczonym;
3. Spełnienie żądań osoby je kierującej nastąpi wyłącznie w przypadkach przewidzianych w Rozporządzeniu, jeżeli nie zachodzą okoliczności uprawniające Szkołę Podstawową do dalszego przetwarzania danych mimo zgłoszonych żądań;
4. Szkoła Podstawowa udzieli odpowiedzi na wystosowane żądanie sprostowania, ograniczenia i usunięcia danych osobowych lub złożony sprzeciw w terminie jednego miesiąca lub dwóch miesięcy w sprawach szczególnie skomplikowanych.

Szkoła Podstawowa ma obowiązek usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

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

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;

d) osoba, której dane dotyczą, wnosi sprzeciw, a jej dane są przetwarzane na potrzeby marketingu bezpośredniego

e) dane osobowe były przetwarzane niezgodnie z prawem;

f) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie krajowym

g) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Szkoła Podstawowa nie ma obowiązku usunąć danych w zakresie w jakim ich przetwarzanie jest niezbędne m.in.:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa krajowego;

c) do ustalenia, dochodzenia lub obrony roszczeń.

Szkoła Podstawowa ma obowiązek ograniczyć przetwarzanie danych osobowych, co należy rozumieć jako zawieszenie przetwarzania, jeżeli:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych - na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

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

c) Szkoła Podstawowa nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

13 Instrukcja dotycząca sposobu zarządzania systemem informatycznym.

Niniejsza instrukcja obejmuje zagadnienia związane z zabezpieczeniem sprzętu informatycznego, danych i oprogramowania, procedury rozpoczęcia i zakończenia pracy ze wskazanym sprzętem, jak również zabezpieczania ich przed nieuprawnionym dostępem i procedurą ich konserwacji oraz przeglądów technicznych.

13.1 Zasady zabezpieczania sprzętu informatycznego, danych i oprogramowania.

Wprowadza się następujące zasady zabezpieczania sprzętu informatycznego, danych i oprogramowania:

1) uwzględniając kategorie przetwarzanych danych osobowych oraz zagrożenia wprowadza się wysoki poziom bezpieczeństwa w systemie informatycznym służącym do przetwarzania danych osobowych,

2) kontroli podlega dostęp do pomieszczeń, w których znajduje się sprzęt komputerowy i szafy z aktami, w celu zabezpieczenia sprzętu oraz danych osobowych i oprogramowania przed ich wykorzystaniem lub zniszczeniem przez osoby trzecie. PBudynek, w którym znajdują się pomieszczenia zamykany jest przez ostatnią osobę go opuszczającą.

3) pracowników obowiązuje bezwzględny zakaz wynoszenia płyt lub innych nośników z oprogramowaniem lub innymi danymi poza teren siedziby jednostki, chyba że zgodę na taką czynność wyrazi Administrator Danych Osobowych.

4) płyty lub inne nośniki z oprogramowaniem lub innymi danymi zabezpieczone są

szyfrowaniem.

5) Administrator Danych Osobowych zobowiązany jest prowadzić ewidencję płyty lub innych nośników z oprogramowaniem lub innymi danymi.

6) dopuszcza się, za zgodą Administratora Danych Osobowych, instalowania programów zawierających dane osobowe na komputerach przenośnych tzw. notebookach. Musi on jednak posiadać zainstalowane mechanizmy ochronne oraz kompleksowe oprogramowanie antywirusowe. Ponadto użytkownik takiego komputera musi dochować wszelkiej staranności, aby zapobiec kradzieży jego komputera przenośnego.

7) urządzenia, dyski lub inne nośniki informacji przeznaczone do:

   a) likwidacji – pozbawia się danych poprzez formatowanie oraz fizyczne uszkodzenie, uniemożliwiające ich odczytanie,

   b) przekazania – pozbawia się zapisu zawierającego dane osobowe,

   c) naprawy – pozbawia się zapisu danych osobowych lub naprawia pod nadzorem osoby do tego upoważnionej przez Administratora Danych Osobowych.

8) na stanowiskach pracy, na których przetwarzane są dane osobowe, ekrany monitorów powinny być ustawione w sposób uniemożliwiający osobom trzecim wgląd w wyświetlane informacje.

9) w razie przerwania pracy stosuje się „wygaszacz ekranu".

10) jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

   a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;

   b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

11) system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

12) logiczne zabezpieczenia chroniące przed nieuprawnionym dostępem obejmują:

   a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;

   b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

13) każdy z komputerów zabezpieczony jest hasłem dostępu, składającym się z co najmniej ośmiu znaków, zawierający małe i wielkie litery oraz cyfry lub znaki specjalne. Każdy z Pracowników ma obowiązek nie rzadziej niż co 30 dni zmiany hasła dostępu do komputera oraz do przekazania go w zamkniętej i w podpisanej kopercie Administratorowi Danych Osobowych, Inspektorowi Ochrony Danych lub Administratorowi Systemów Informatycznych.

14) nieaktualne koperty z hasłami są niszczone przez Administratora Danych Osobowych, Inspektora Ochrony Danych lub Administratora Systemów Informatycznych za pomocą niszczarki.

15) stosuje się środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

13.2 Procedura rozpoczęcia i zakończenia pracy.

Wprowadza się następujące procedury rozpoczęcia i zakończenia pracy ze sprzętem informatycznym:

1) komputer uruchamia się po wprowadzeniu do niego hasła,
2) przy wejściu do systemu przetwarzającego dane osobowe wprowadza się identyfikator oraz hasło dostępu,
3) zakończenie pracy związanej z przetwarzaniem danych odpowiadać winno wszystkim regułom bezpieczeństwa informacji.

13.3 Zabezpieczenie systemu przed nieuprawnionym dostępem.

W celu zabezpieczenia systemu przed nieuprawnionym dostępem:

1) dopuszcza się możliwość przyłączenia sieci internetowej do systemu, w którym przetwarzane są dane osobowe pod następującymi warunkami:

a) na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe,

b) każdy e-mail wpływający do jednostki musi być sprawdzony pod kątem występowania wirusów,

c) aktualizacje programów antywirusowych muszą być dokonywane nie rzadziej niż raz w tygodniu,

d) zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym, którego dokonuje użytkownik zamierzający go użyć,

e) zabrania się pobierania z Internetu plików niewiadomego pochodzenia oraz odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym,

- powyższe informacje mogą ulec zmianie ze względu na pracę danego oprogramowania antywirusowego za co nie ponosi odpowiedzialności Administrator Danych Osobowych.

2) każdy Użytkownik systemu musi zostać przeszkolony z obsługi programu antywirusowego.

3) Administrator Danych Osobowych, Inspektor Ochrony Danych lub Administrator Systemów Informatycznych przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach systemu przynajmniej raz na 3 miesiące.

4) Użytkownicy systemu są odpowiedzialni za nieudostępnianie stanowisk pracy osobom postronnym.

13.4 Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

Wprowadza się następujące procedury naprawy i przeglądu sprzętu komputerowego i systemu:

1) procedury naprawy sprzętu komputerowego:

Naprawa sprzętu komputerowego użytkowanego w systemie może dokonywać jedynie wyspecjalizowany podmiot świadczący usług informatyczne w siedzibie Administratora Danych Osobowych lub w siedzibie danego podmiotu. Czynności wykonywane w siedzibie Administratora Danych Osobowych odbywają się w obecności osoby wskazanej przez Administratora Danych Osobowych, Inspektora Ochrony Danych, Administratora Systemów Informatycznych lub upoważnionego przez nich Użytkownika systemu.

2) procedura przeglądu systemu:
   a) przeglądu systemu dokonuje wyspecjalizowany podmiot świadczący usług informatyczne,
   b) czynności przeglądowe muszą odbywać się w obecności Administratora Danych Osobowych, Inspektora Ochrony Danych lub Administratora Systemów Informatycznych lub upoważnionego przez nich Użytkownika systemu.

14 Wydruki.

Odnośnie zabezpieczenia papierowej wersji danych osobowych wprowadza się następujące zasady:

1) wydruki, kartoteki oraz dokumenty papierowe, na których znajdują się dane osobowe, są w szafach, w sposób uniemożliwiający wgląd przez nieupoważnione osoby trzecie.
2) wydruki zawierające dane osobowe przeznaczone do usunięcia niszczy się w niszczarce, natomiast inne przechowywane są w warunkach uniemożliwiających dostęp do nich nieupoważnionych osób trzecich.
3) pomieszczenia, w których przechowywane są wydruki zawierające dane osobowe musi być należycie zabezpieczone po godzinach pracy.

15 Załączniki.

Załącznik nr 1 – Opis struktury zbiorów danych wraz z zawartością poszczególnych pół informacyjnych i istniejących pomiędzy nimi powiązań.

Załącznik nr 2 – Opis obszarów, w których przetwarzane są dane osobowe.

Załącznik nr 3 – Opis przepływu danych osobowych.

Załącznik nr 4a – Środki ochrony technicznej i fizycznej niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Załącznik nr 4b – Środki organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Załącznik nr 5 – Ustanowienie Inspektora Ochrony Danych.

Załącznik nr 6 – Upoważnienie Inspektora Ochrony Danych do nadawania upoważnień.

Załącznik nr 7 – Ustanowienie Administratora Systemów Informatycznych.

Załącznik nr 8a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę.

Załącznik nr 8b – Wzór upoważnienia do przetwarzania danych osobowych dla osób

zatrudnionych na podstawie umowy innej niż umowa o pracę

Załącznik nr 9 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

Załącznik nr 10 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 11 Wykaz podmiotów, którym Administrator Danych Osobowych powierzył przetwarzanie danych osobowych

Załącznik nr 12 – Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających

Załącznik nr 13 – Wzór informacji dotyczących przetwarzania danych osobowych wraz wykazem lokalizacji i sposobów jej udostępniania.

……

data i podpis osoby reprezentującej
Administratora Danych Osobowych

Załącznik nr 1 – Opis struktury zbiorów danych wraz z zawartością poszczególnych pół informacyjnych i istniejących pomiędzy nimi powiązań.

Lp.	Nazwa zbioru	Sposób przetwarzania danych	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Powiązania z innymi zbiorami danych	Podstawa prawna	Planowany termin usunięcia	Podmiot przetwarzający
1.	Dane uczniów - dziennik	elektroniczny	1) realizacja programu nauczania 2) realizacja obowiązku szkolnego, ewidencjonowanie przebiegu procesu edukacji 3)	Uczniowie	Imię i nazwisko,	Powiązanie ze zbiorami: 1) Dane uczniów zajęcia dodatkowe (elektroniczne i papierowe)	- obowiązki wynikające z rozporządzenia Ministra Edukacji Narodowej z dnia 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji	Upływ terminów przewidzianych ustawowo do celów prowadzenia dokumentacji.	Podmiot wskazany w wykazie podmiotów przetwarzających, którego wzór stanowi Załącznik nr 11 do Polityki Bezpieczeństwa – poz. 1
2.	Dane uczniów zajęcia dodatkowe (dokumentowe)	papierowy	1) realizacja zdań statutowych	Uczniowie	Imię i nazwisko	Powiązanie ze zbiorami: 1) Dane uczniów zajęcia dodatkowe (elektroniczne)	- wykonanie obowiązków nałożonych przez radę pedagogiczną w związku z zadaniami określonymi w statucie szkoły.	Upływ terminów przewidzianych ustawowo do celów prowadzenia dokumentacji.	Brak

3.	Dane uczniów zajęcia dodatkowe (elektroniczne)	papierowy	1) realizacja zadań statutowych	Uczniowie	Imię i nazwisko	Powiązanie ze zbiorami: 1) Dane uczniów zajęcia dodatkowe (papierowe)	- wykonanie obowiązków nałożonych przez radę pedagogiczną w związku z zadaniami określonymi w statucie szkoły.	Upływ terminów przewidzianych ustawowo do celów prowadzenia sprawozdawczości	Podmiot wskazany w wykazie podmiotów przetwarzających, którego wzór stanowi Załącznik nr 11 do Polityki Bezpieczeństwa – poz. 1
4.	Dane Systemu Informacji Oświatowej (SIO)	elektroniczny	1)informowanie o sposobie zarządzania placówką 2) wykorzystaniu środków przeznaczonych na realizację zadań oświatowych 3) kontrolowanie jakości edukacji	Uczniowie	Imię i nazwisko ucznia, stan zdrowia ucznia, numer PESEL, Imiona i nazwiska rodziców, numery PESEL rodziców, adresy zamieszkania rodziców, informacje związane z trasa dojazdu ucznia i kosztami	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik 2) Dane uczniów zajęcia dodatkowe (elektroniczne i papierowe) 3) Dane pedagogiczne (dokumentowe) 4)Dane pedagogiczne (elektroniczne) 5)Dziennik nauczania indywidualnego 6)Dziennik logopedy	- wykonanie zadań ustawowych określonych ustawą o systemie informacji oświatowej.	Upływ terminów przewidzianych ustawowo do celów prowadzenia sprawozdawczości	Podmiot wskazany w wykazie podmiotów przetwarzających, którego wzór stanowi Załącznik nr 11 do Polityki Bezpieczeństwa – poz. 1
5.	Zeszyt wychowawcy	papierowy	1) zapewnienie bezpośredniego kontaktu z opiekunami prawnymi uczniów.	Uczniowie	Imię i nazwisko, PESEL ucznia, imiona rodziców numer telefonu do rodziców	Powiązanie ze zbiorami: brak	- wykonanie prawnie uzasadnionych interesów przez administratora –wykonywanie zadań ustawowych	Do czasu zakończenia edukacji przez Ucznia	Brak

							określonych ustawą o systemie informacji oświatowej - zapewnienie kontaktu z opiekunami prawnymi.		
6.	Dane sprawozdawcze z rady pedagogicznej (papierowe)	papierowe	1)zapewnienie decyzyjności w bieżących sprawach szkoły.	Uczniowie i Pracownicy	Imię i nazwisko, dane wrażliwe adresy?	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik 2) Dane uczniów zajęcia dodatkowe (elektroniczne i papierowe)	Realizacja zadań określonych w systemie aktów prawnych z zakresu prawa oświatowego uszczegółowionych w statucie szkoły.	Upływ terminów przewidzianych ustawowo.	Brak
7.	Dane rekrutacyjne (dokumentowe)	papierowy	1)prowadzenie procesu rekrutacji	Uczniowie	Imię i nazwisko, firma działalności gospodarczej (jeżeli posiada), adres e-mail	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik	Realizacja obowiązków ustawowych z zakresu oświaty	Upływ terminów przewidzianych ustawowo	Brak
8.	Dane rekrutacyjne (elektroniczne)	elektroniczne	prowadzenie procesu rekrutacji	Uczniowie	Imię i nazwisko, firma działalności gospodarczej (jeżeli posiada), adres e-mail	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik	Realizacja obowiązków ustawowych z zakresu oświaty	Upływ terminów przewidzianych ustawowo.	Podmiot wskazany w wykazie podmiotów przetwarzających, którego wzór stanowi Załącznik nr 11 do Polityki Bezpieczeństwa – poz. 1

9.	Dane pedagogiczne (dokumentowe)	papierowe	Udzielanie pomocy pedagogicznej	Uczniowie, Rodzice	Imię i nazwisko, stan zdrowia	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik 2) Dane pedagogiczne (dokumentowe) 3)Dane pedagogiczne (elektroniczne) 4)Dziennik nauczania indywidualnego 5)Dziennik logopedy	Realizacja zadań określonych w systemie aktów prawnych z zakresu prawa oświatowego uszczegółowionych w statucie szkoły	Upływ terminów przewidzianych ustawowo.	Brak
10.	Dane pedagogiczne (elektroniczne)	elektroniczne	Udzielanie pomocy pedagogicznej	Uczniowie, Rodzice	Imię, nazwisko, numer opinii, orzeczenie, stan zdrowia	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik 2) Dane pedagogiczne (dokumentowe) 3)Dane pedagogiczne (elektroniczne) 4)Dziennik nauczania indywidualnego 5)Dziennik logopedy	Realizacja zadań określonych w systemie aktów prawnych z zakresu prawa oświatowego uszczegółowionych w statucie szkoły	Upływ terminów przewidzianych ustawowo.	Podmiot wskazany w wykazie podmiotów przetwarzających, którego wzór stanowi Załącznik nr 11 do Polityki Bezpieczeństwa – poz. 1
11.	Wykaz legitymacji	papierowa	Ewidencjonowanie osób uczęszczających do szkoły i podlegających obowiązkowi szkolonemu, potwierdzenie	Uczniowie	Imię i nazwisko, PESEL	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik	Realizacja zadań określonych w systemie aktów prawnych z zakresu prawa oświatowego uszczegółowionych w statucie szkoły	Upływ terminów przewidzianych ustawowo.	Brak

			uprawnień ustawowych wynikających ze statusu ucznia						
12.	Wykaz świadectw	papierowa	Ewidencjonowanie świadectw rocznych i ukończenia szkoły	Uczniowie	Imię i nazwisko	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik	Realizacja zadań określonych w systemie aktów prawnych z zakresu prawa oświatowego uszczegółowionych w statucie szkoły	Upływ terminów przewidzianych ustawowo.	Brak
13.	Wykaz świadectw	elektroniczne	Ewidencjonowanie świadectw rocznych i ukończenia szkoły	Uczniowie	Imię i nazwisko	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik	Realizacja zadań określonych w systemie aktów prawnych z zakresu prawa oświatowego uszczegółowionych w statucie szkoły	Upływ terminów przewidzianych ustawowo.	Podmiot wskazany w wykazie podmiotów przetwarzających, którego wzór stanowi Załącznik nr 11 do Polityki Bezpieczeństwa – poz. 1
14.	Dziennik logopedy	papierowa	Udzielenia pomocy logopedycznej, wykonywanie świadczeń medycznych	Uczniowie	Imię nazwisko, Dane wrażliwe dotyczące stanu zdrowia	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik 2) Dane pedagogiczne (dokumentowe) 3)Dane pedagogiczne (elektroniczne)	Realizacja zadań określonych w systemie aktów prawnych z zakresu prawa oświatowego uszczegółowionych w statucie szkoły	Upływ terminów przewidzianych ustawowo.	Brak

15.	Wykaz zaświadczeń odbioru wyników egzaminów	papierowa	Prowadzenie ewidencji odebranych zaświadczeń	Uczniowie, Rodzice	Imię i nazwisko	Powiązanie ze zbiorami: 1) Dane uczniów - dziennik	Realizacja zadań określonych w systemie aktów prawnych z zakresu prawa oświatowego	Upływ terminów przewidzianych ustawowo.	Brak
16.	Dane fakturowe (elektroniczne)	elektroniczny	prowadzenie sprawozdawczości finansowej i realizacja płatności	Kontrahenci	Imię i nazwisko, adres zamieszkania, NIP (jeśli posiada), adres prowadzenia działalności gospodarczej (jeżeli posiada), firma działalności gospodarczej (jeżeli posiada), numer telefonu, e-mail	Powiązanie ze zbiorami: 1) Dane fakturowe (dokumentowe) 2)Dane kontrahentów papierowe	- wykonanie umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy - wypełnienie obowiązku prawnego przewidzianego przepisami prawa podatkowego oraz ustawy o rachunkowości	Upływ terminów przewidzianych ustawowo do celów prowadzenia sprawozdawczości finansowej.	Podmiot wskazany w wykazie podmiotów przetwarzających, którego wzór stanowi Załącznik nr 11 do Polityki Bezpieczeństwa – poz. 1
17.	Dane ofertowe	papierowe	1) realizacja zamówień, przetargów, ocena ofert	Kontrahenci	Imię i nazwisko, numer telefonu, adres e-mail, adres zamieszkania, adres do dostawy, NIP (jeżeli posiada), adres	Powiązanie ze zbiorami: 1)Dane fakturowe (dokumentowe): 2)Dane fakturowe (elektroniczne): 3)Dane Kontrahentów 4) Dane ofertowe elektroniczne.	- realizacja postępowań w celu zawarcia umowy z podmiotem trzecim zgodnie z wymogami prawa zamówień publicznych	Na czas realizacji umowy i przedawnienia roszczeń związanych z ewentualnymi sporami.	Brak

					prowadzenia działalności gospodarczej (jeżeli posiada), firma działalności gospodarczej (jeżeli posiada)				
18.	Dane archiwizacyjne	papierowe	1) gromadzenie, przechowywanie dokumentacji do celów ewidencyjnych i kontrolnych	Uczniowie i Rodzice	Imię i nazwisko ucznia, stan zdrowia ucznia, numer PESEL, Imiona i nazwiska rodziców, numery PESEL rodziców, adresy zamieszkania rodziców, informacje związane z trasa dojazdu ucznia i kosztami	Powiązanie ze wszystkimi zbiorami od 1-24 oraz 26-27.	Realizacja zadań określonych w systemie aktów prawnych z zakresu prawa oświatowego oraz innych właściwych aktów prawnych.	Upływ terminów przewidzianych ustawowo do celów archiwizacji.	Brak
19.	Dane z monitoringu	elektroniczne	1)zapewnienie bezpieczeństwa na terenie objętym monitoringiem	Uczniowie, Pracownicy, Kontrahenci, Osoby trzecie	Zapis elektroniczny wizji.	Powiązanie ze zbiorami: brak.	Realizacja prawnie uzasadnionych interesów administratora	Przechowywanie do 3 miesięcy.	Brak

20.	Dane pracownicze (dokumentowe)	papierowy	1)prowadzenie spraw kadrowych, 2)zapłata wynagrodzeń pracowniczych.	Pracownicy	Imię i nazwisko, adres zamieszkania, numer PESEL, numer dowodu osobistego, numer prawa jazdy	Powiązanie ze zbiorami: 1)Dane pracownicze elektroniczne	-wykonanie umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy -wypełnienie obowiązku prawnego przewidzianego przepisami prawa podatkowego oraz prawa pracy	Upływ terminów ustawowych przewidzianych w przepisach prawa pracy	Brak
21.	Dane biblioteczne (dokumentowe)	papierowe	1)prowadzenie ewidencji związanej z udostępnienie m zbiorów biblioteki szkolnej.	Uczniowie	Imię i nazwisko, adres zamieszkania	Powiązanie ze zbiorami: 1) Dane uczniów – dziennik 2) Dane biblioteczne elektroniczne	Realizacja obowiązków ustawowych w zakresie prowadzenia ewidencji związanej z udostępnieniem zbiorów biblioteki szkolnej	Upływ terminów określonych przepisami prawa w tym ustawą o bibliotekach.	Brak

22.	Dane biblioteczne (elektroniczne)	elektroniczne	1)prowadzenie ewidencji związanej z udostępnienie m zbiorów biblioteki szkolnej.	Uczniowie	Imię i nazwisko, adres zamieszkania	Powiązanie ze zbiorami: 1) Dane uczniów – dziennik 2) Dane biblioteczne papierowe	Realizacja obowiązków ustawowych w zakresie prowadzenia ewidencji związanej z udostępnieniem zbiorów biblioteki szkolnej	Upływ terminów określonych przepisami prawa w tym ustawą o bibliotekach.	Podmiot wskazany w wykazie podmiotów przetwarzającyc h, którego wzór stanowi Załącznik nr 11 do Polityki Bezpieczeństwa – poz. 1

Załącznik nr 2 – Obszary, w których przetwarzane są dane osobowe.

Siedziba Szkoły znajduje się w miejscowości Bilcza 75.. W budynku Szkoły Podstawowej przechowywana jest cała dokumentacja, w której przetwarzane są dane osobowe.

Przetwarzanie danych osobowych odbywa się w celach edukacyjnych, kadrowych, finansowych

Ponadto przetwarzanie danych osobowych wyłącznie celach sprawozdawczości finansowej oraz w związku z zatrudnieniem odbywa się również przez wewnętrzny dział księgowości.

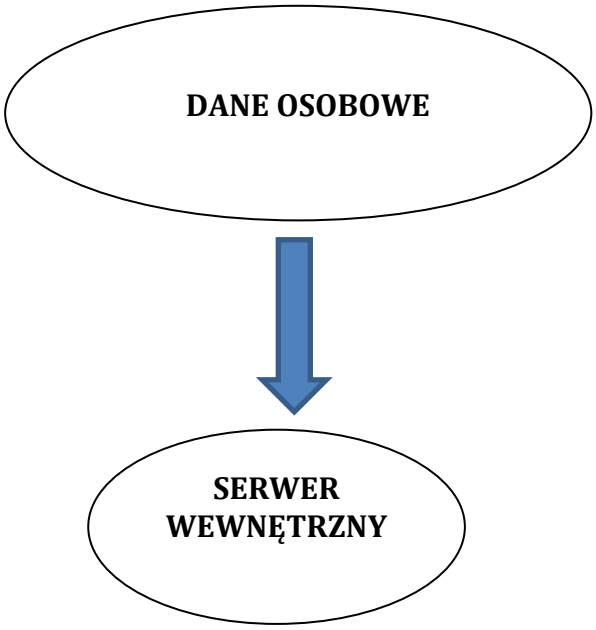
Dane w wersji papierowej przechowywane są w szafach zamykanych na klucz, znajdujących się w budynku Szkoły Podstawowej w Bilczy w odrębnym pomieszczeniu zamykanym na klucz. Budynek jest monitorowany, jest wyposażony w alarm, przed budynkiem znajduje się brama wjazdowa.

Wszystkie pomieszczenia w Budynku chronione są drzwiami zamykanymi na klucz oraz oknami.

Załącznik nr 3 – Opis przepływu danych osobowych.

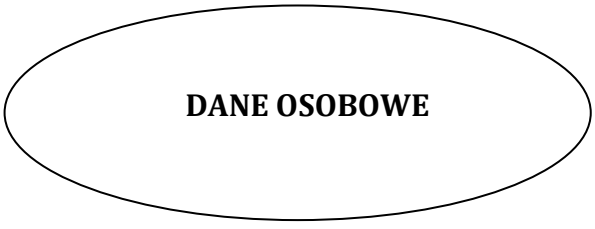
1)Dane uczniów – dziennik, Dane rekrutacyjne (elektroniczne), Dane pedagogiczne (elektroniczne), Wykaz świadectw, Dane biblioteczne(elektroniczne), Dane uczniów zajęcia dodatkowe.

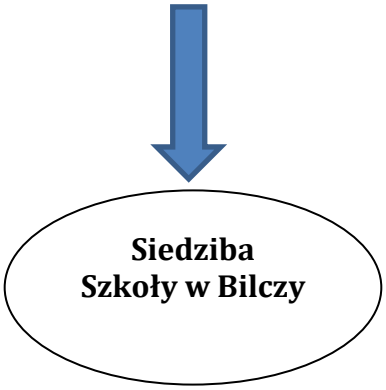
a) dane przechowywane i przetwarzane są w siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów;
b) dane przechowywane i przetwarzane są również na serwerze, dyskach zewnętrznych,
c) sporządzenie aktualizacji ww. danych należy do obowiązków Szkoły
d) konserwacja serwerów należy do obowiązków profesjonalnego podmiotu świadczącego usługi informatyczne.



2) Dane uczniów zajęcia dodatkowe (dokumentowe) Zeszyt wychowawcy, Dane sprawozdawcze z rady pedagogicznej (papierowe), Dane rekrutacyjne (dokumentowe), Dane pedagogiczne (dokumentowe), Wykaz legitymacji, Wykaz świadectw, Dziennik logopedy, Wykaz zaświadczeń odbioru wyników egzaminów, Dane archiwizacyjne, Dane biblioteczne(dokumentowe).

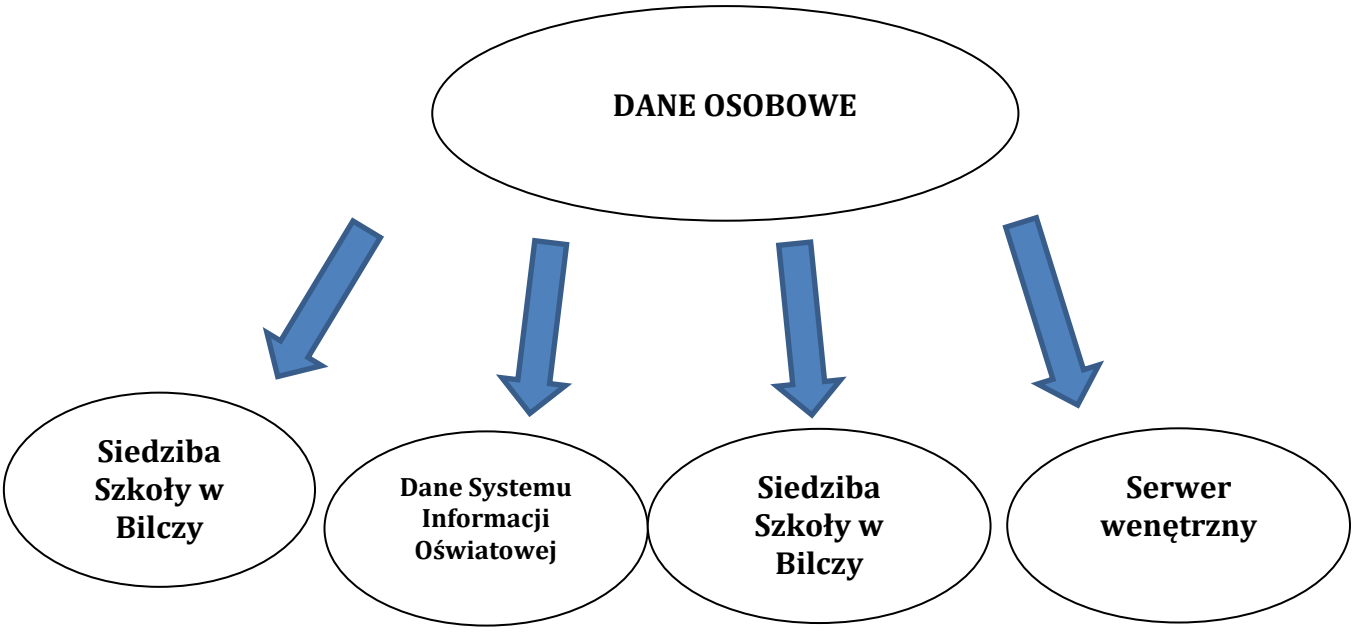
a) dane przechowywane i przetwarzane są w siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów.





3)Dane Systemu Informacji Oświatowej (SIO)

a) dane przechowywane i przetwarzane są w siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów;
b) dane przechowywane i przetwarzane są również na serwerze, dyskach zewnętrznych,
c) sporządzenie aktualizacji ww. danych należy do obowiązków Szkoły
d) konserwacja serwerów należy do obowiązków profesjonalnego podmiotu świadczącego usługi informatyczne na podstawie wiążącej go ze Szkołą umowy.

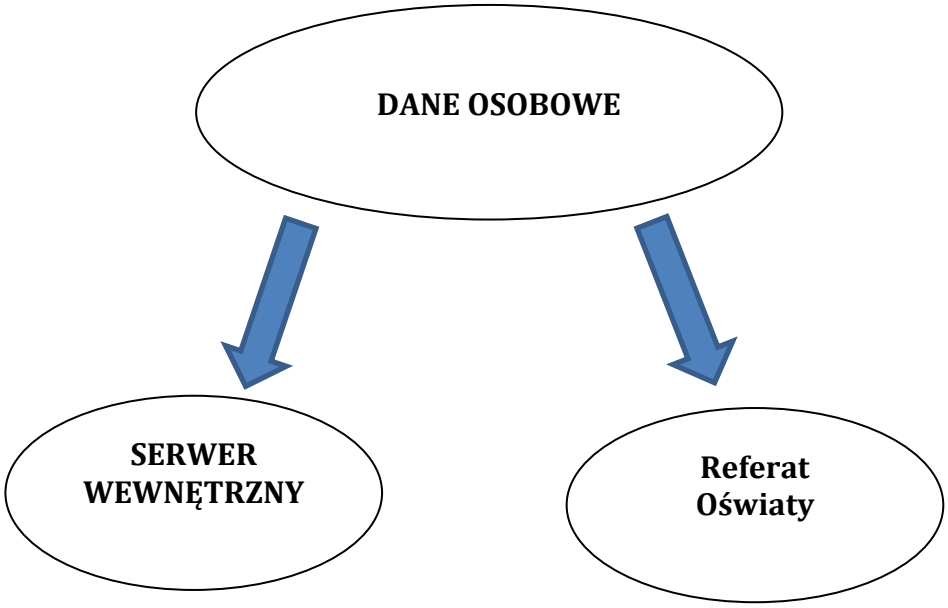


4) Dane Kontrahentów (elektroniczne i papierowe),

a) dane przechowywane i przetwarzane są w siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów;
b) dane przechowywane i przetwarzane są również na serwerze, dyskach

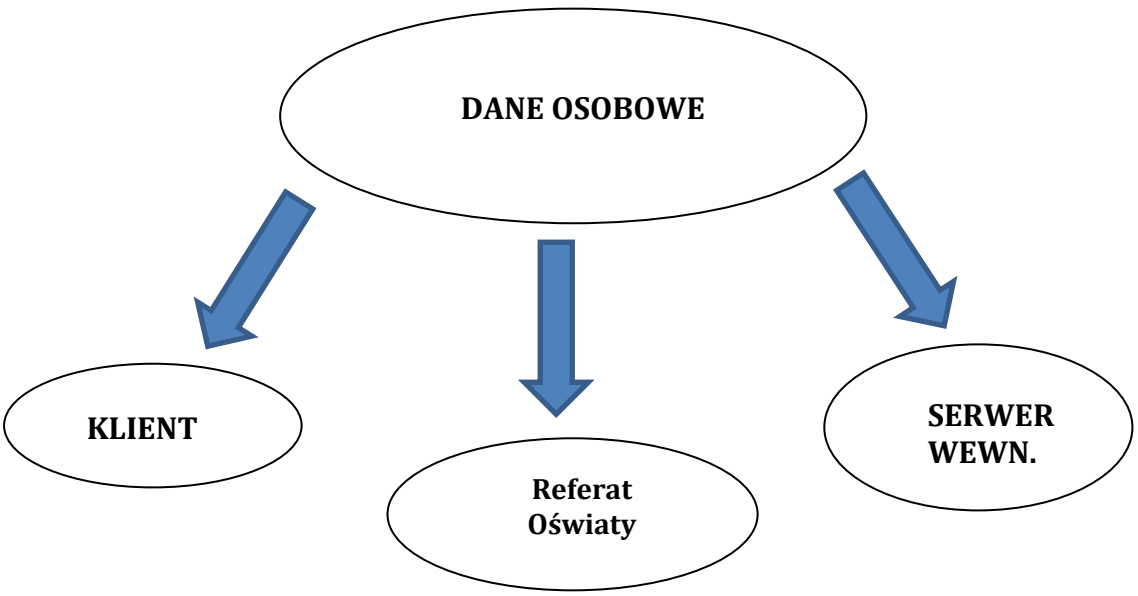
zewnętrznych,

c) sporządzenie aktualizacji ww. danych należy do obowiązków Szkoły
d) konserwacja serwerów należy do obowiązków profesjonalnego podmiotu świadczącego usługi informatyczne.



5) Dane fakturowe klientów (elektroniczne)

a) dane przechowywane i przetwarzane są w siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów;
b) dane przechowywane i przetwarzane są również na serwerze, dyskach zewnętrznych,
c) sporządzenie aktualizacji ww. danych należy do obowiązków Szkoły
d) konserwacja serwerów należy do obowiązków profesjonalnego podmiotu świadczącego usługi informatyczne na podstawie wiążącej go ze Szkołą umowy.

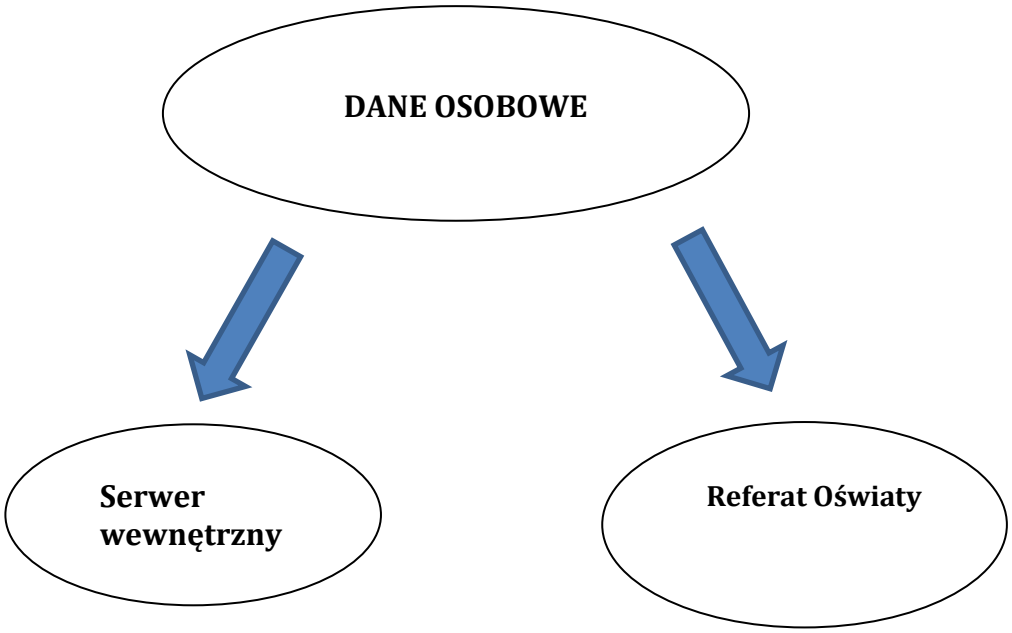


6) Dane fakturowe klientów (papierowe)

a) dane przechowywane i przetwarzane są siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów;
b) dane przechowywane i przetwarzane są również na serwerze, dyskach zewnętrznych,
c) sporządzenie aktualizacji ww. danych należy do obowiązków Szkoły
d) konserwacja serwerów należy do obowiązków profesjonalnego podmiotu świadczącego usługi informatyczne.

7) Dane pracownicze (elektroniczne i papierowe)

a) dane przechowywane i przetwarzane są w siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów;
b) dane przechowywane i przetwarzane są również na serwerze, dyskach zewnętrznych,
c) sporządzenie aktualizacji ww. danych należy do obowiązków Szkoły
d) konserwacja serwerów należy do obowiązków profesjonalnego podmiotu świadczącego usługi informatyczne;



8) Dane ofertowe dokumentowe

a) dane przechowywane i przetwarzane są w siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów;

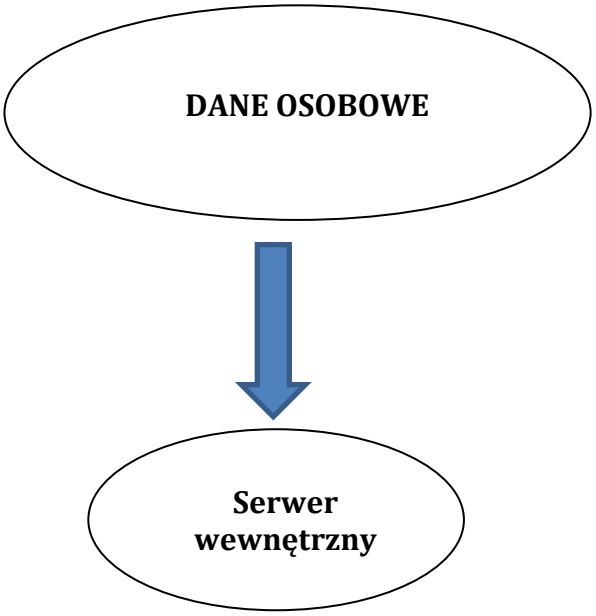
9) Dane ofertowe elektroniczne

a) dane przechowywane i przetwarzane są w siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy;
b) dane przechowywane i przetwarzane są również na serwerze, dyskach zewnętrznych,

c) sporządzenie aktualizacji ww. danych należy do obowiązków Szkoły
d) konserwacja serwerów należy do obowiązków profesjonalnego podmiotu świadczącego usługi informatyczne .

10) Dane z monitoringu

a) dane przechowywane i przetwarzane są również na serwerze, dyskach zewnętrznych;



Załącznik nr 4a – Środki ochrony technicznej i fizycznej niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

L.p.	Środek ochrony technicznej i fizycznej
1.	Zbiór danych osobowych w formie elektronicznej ma zabezpieczenie w postaci hasła i loginu.
3.	Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych są pod nadzorem Pracowników.
4.	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej na klucz szafie lub w pomieszczeniu, zamykanym na klucz.
5.	Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej na klucz szafie lub pomieszczeniu, zamykanym na klucz.
6.	Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i wolnostojącej gaśnicy.
7.	Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
8.	Zastosowano system monitoringu.
9.	Zastosowano odseparowanie od sieci publicznej danych elektronicznych – tzw. firewall.
10.	Poczta elektroniczna e- mail łączy się przez SSL (połączenie zabezpieczone).
11.	Hasła na komputerach zmieniane są co 30 dni i zawierają minimum 8 znaków, wielka litera, znak cyfrowy lub specjalny.
12.	Naprawa komputera następuje na miejscu, dane z dysku twardego takiego komputera kopiowane są na obcy drugi komputer z danego działu.
13.	Kopie baz danych wykonywane są raz dziennie, a plików rozproszonych raz w tygodniu.
14.	W przypadku awarii serwera jest on naprawiany za pośrednictwem archiwizatora zewnętrznego.
15.	Istnieje możliwość skorzystania ze wsparcia technicznego (support) firmy zewnętrznej tworzącej oprogramowanie.
16.	W przypadku awarii komputera nie objętego gwarancją, przed oddaniem do naprawy dysk jest fizycznie niszczony (przewiercanie). W przypadku gdy komputer podlega gwarancji dysk podlega celowej demagnetyzacji.
17.	Urządzenia przenoszące dane na zewnątrz oraz cały sprzęt komputerowy jest zaewidencjonowany i zaszyfrowany.
18.	W przypadku zgubienia lub uszkodzenia urządzenia przenoszącego dane jest to zgłaszane niezwłocznie Administratorowi Danych Osobowych.

Załącznik nr 4b – Środki organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

L.p.	Środek organizacyjny
1.	Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.
2.	Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
4.	Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych.
5.	Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
6.	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
7.	Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
8.	Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
9.	Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.
10.	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.

Załącznik nr 5 – Ustanowienie Inspektora Ochrony Danych.

Niniejszym, **<u>wyznaczam</u>**

Panią/Pana ……..

na stanowisko **Inspektora Ochrony Danych (dalej jako „IOD")** siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów; Zakres obowiązków oraz warunki pełnienia funkcji Inspektora Ochrony Danych określone są w Ogólnym Rozporządzeniu o Ochronie Danych oraz dokumentacją z zakresu ochrony danych osobowych wdrożoną dnia ……..w Szkole.

data i podpis osoby wyznaczonej na stanowisko IOD	data i podpis osoby reprezentującej Administratora Danych Osobowych

Załącznik nr 6 – Upoważnienie Inspektora Ochrony Danych do nadawania upoważnień

Niniejszym, reprezentując i działając w imieniu Administratora Danych Osobowych siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów; **upoważniam**

Panią/Pana ……..

Inspektora Ochrony Danych (dalej jako „IOD") w siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów; do nadawania w imieniu Administratora Danych Osobowych upoważnień do przetwarzania danych osobowych.

data i podpis osoby wyznaczonej na stanowisko IOD	data i podpis osoby reprezentującej Administratora Danych Osobowych

Załącznik nr 7 – Ustanowienie Administratora Systemów Informatycznych

Niniejszym, reprezentując i działając w imieniu Administratora Danych Osobowych siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów; **wyznaczam**

Panią/Pana ……..

na stanowisko **Administratora Systemów Informatycznych (dalej jako: „ASI")** siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów; Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone są dokumentacją z zakresu . ochrony danych osobowych wdrożoną dnia ……. w Szkole.

data i podpis osoby wyznaczonej na stanowisko ASI

data i podpis osoby reprezentującej Administratora Danych Osobowych

Załącznik nr 8a – wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

U P O W A Ż N I E N I E D O P R Z E T W A R Z A N I A D A N Y C H O S O B O W Y C H

Niniejszym, jako działając w imieniu siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów; (dalej jako Szkoła) **upoważniam do przetwarzania danych osobowych:**

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych Osobowych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ogólnego Rozporządzenia o Ochronie Danych, wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Szkoły wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności na gruncie ww. rozporządzenia oraz ustawy o ochronie danych osobowych.

Upoważnienie jest ważne do odwołania.

....

data i podpis upoważniającego data i podpis osoby upoważnionej

---

OŚWIADCZENIE

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Szkole (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....

data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Załącznik Nr 8b – wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie innej umowy niż umowa o pracę

U P O W A Ż N I E N I E D O P R Z E T W A R Z A N I A D A N Y C H O S O B O W Y C H

Niniejszym, działając w imieniu siedzibie Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów; (dalej jako Szkoła), **upoważniam do przetwarzania danych osobowych:**

Imię i nazwisko upoważnionego	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ogólnego Rozporządzenia o Ochronie Danych, wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Szkole wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności na gruncie ww. rozporządzenia oraz ustawy o ochronie danych osobowych.

Upoważnienie jest ważne do odwołania.

data i podpis upoważniającego

data i podpis osoby upoważnionej

OŚWIADCZENIE

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Szkole (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych w związku z pełnioną przeze mnie funkcją i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu stosunku prawnego łączącego mnie z Administratorem Danych Osobowych.

……..

data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:

1 x oryginał dokumentacja kadrowa

1 x oryginał osoba upoważniona

Załącznik nr 9 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

…………………., dnia …………….

OŚWIADCZENIE O ZOBOWIĄZANIU SIĘ DO ZACHOWANIA POUFNOŚCI

Ja niżej podpisana/y . . . . zamieszkała/y w . . . . zatrudniona/y na stanowisku . . . . zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z ………………………….. Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

……………………….……………………..

podpis i data

Załącznik nr 10 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Nazwy zbiorów objętych zakresem upoważnienia
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				

Załącznik nr 11 – Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych

	Adres / lokalizacja	**Uwagi**
Podmioty, którym Administrator Danych Osobowych powierzył przetwarzanie danych osobowych	Damian Sadok, sadok@interia.pl	

Załącznik nr 12 - Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/ czynności sprawdzających

……., dnia ……

PROTOKÓŁ

Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH

w zakresie ochrony danych osobowych

1. Nazwa kontrolowanej jednostki organizacyjnej:……
2. Zbiory danych osobowych, których przetwarzanie podlega kontroli: ……
   ……
3. Data wykonania czynności kontrolnych:……
4. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne: ……
5. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej:

……
……
……

6. Ustalenia dokonane w trakcie czynności kontrolnych:

……
……
……
……
……
……

7. Wnioski i zalecenia pokontrolne:

……
……
……
……
……
……

…….. ……..

data i podpis osoby wykonującej czynności kontrolne

data i podpis kierownika kontrolowanej jednostki

Otrzymują:
1 x Kierownik kontrolowanej jednostki organizacyjnej
1 x Inspektor Ochrony Danych

Załącznik nr 13 – Wzór informacji dotyczących przetwarzania danych osobowych wraz wykazem lokalizacji i sposobów jej udostępniania.

OCHRONA DANYCH OSOBOWYCH

Publicznej Szkoły Podstawowej im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów;

INFORMACJA DLA PODMIOTÓW, KTÓRYCH DANE OSOBOWE SĄ PRZETWARZANE

Publiczna Szkoła Podstawowa im. św. Jadwigi Królowej w Bilczy, Bilcza 75, 27-641 Obrazów; (dalej jako „Szkoła") zgodnie z obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) jest administratorem danych osobowych i zapewnia wykorzystanie danych w sposób zgodny z umową, bezpieczny oraz obowiązującymi przepisami prawa.

1. Cel przetwarzania danych osobowych

Dane osobowe podmiotów są przetwarzane w następujących celach:

1) wykonywania obowiązków dydaktyczno – wychowawczych określonych w szczególnych ustawach dotyczących systemu oświaty;
2) zawarcia i wykonywania umów o świadczenie usług lub wykonanie dzieła na rzecz Szkoły;
3) prowadzenia sprawozdawczości finansowej i spraw kadrowych.

Dane osobowe będą przetwarzane przez czas:

1) realizacji zadań ustawowych w celach prawnie uzasadnionych;
2) realizacji umowy i rozliczeń po jej zakończeniu;
3) wykonywania obowiązków rachunkowych, księgowych oraz podatkowych, prowadzenia spraw kadrowych.

2. Kategorie przetwarzanych danych osobowych

Szkoła przetwarza dane podstawowe takie jak imię, nazwisko, PESEL, miejsce

zamieszkania, imiona rodziców nr telefonu, adres e-mail, oraz dane wrażliwe, w tym informacje o stanie zdrowia w celach opisanych w pkt. 1.

3. Podmioty, którym przekazywane są dane osobowe:

Dane osobowe, które są przetwarzane są przekazywane:

1) sądom, urzędom, lub organom prowadzącym postępowanie przygotowawcze celem realizacji uprawnień ustawowych;
2) służbom ratowniczym, prewencyjnym i medycznym wykonującym swoje obowiązki;
3) podmiotom prowadzącym działalność pocztową lub kurierską;

4. Uprawnienia podmiotów, których dane są przetwarzane

1) sprostowanie – prawo do żądania poprawienia nieprawidłowych danych osobowych bądź uzupełnienia danych niekompletnych;
2) usunięcie – żądanie usunięcia danych w określonych okolicznościach:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b) osoba, której dane dotyczą, cofnęła zgodę na przetwarzanie danych osobowych i nie ma innej podstawy prawnej przetwarzania;
   c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania danych osobowych i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba
   d) dane osobowe były przetwarzane niezgodnie z prawem;
   e) w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
   f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego;
3) ograniczenie przetwarzania danych osobowych - żądanie wstrzymania przetwarzania danych osobowych w następujących okolicznościach:
   a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – wstrzymanie następuje na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
d) osoba, której dane dotyczą, wniosła sprzeciw przetwarzania ograniczenie następuje do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Zgłoszenie uprawnień następuje w drodze pisemnej poprzez złożenie stosownego wniosku do podmiotu przetwarzającego dane osobowe.

5. Zgoda.

W przypadku, gdy przetwarzanie danych osobowych nie jest konieczne do wykonywania umowy, nie wynika z przepisów prawa lub nie ma innego uzasadnionego prawnie interesu, podmiot przetwarzający dane osobowe może domagać się wyrażania zgody podmiotów, których dane są przetwarzane we wskazanych przez przetwarzającego dane celach. Osoby, których dane są przetwarzane mają prawo do wycofania zgody na przetwarzanie danych.

6. Prawo do wniesienia sprzeciwu.

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych z przyczyn związanych z jej szczególną sytuacją. Osoba której dane są przetwarzane ma prawo wniesienia sprzeciwu również w zakresie danych, które są przetwarzane na potrzeby marketingu bezpośredniego.
Z chwilą zgłoszenia sprzeciwu podmiotowi przetwarzającemu dane nie wolno już przetwarzać tych danych osobowych. W przypadku wykazania przez podmiot przetwarzający dane osobowe istnienia ważnych prawnie uzasadnionych podstaw do przetwarzania, które jednocześnie są nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą będzie możliwe dalsze przetwarzanie danych osobowych.

7. Skarga. Organ nadzoru.

Osoby, których dane osobowe są przetwarzane mają prawo wnieść skargę do Prezesa

Urzędu Ochrony Danych Osobowych, w przypadku stwierdzenia naruszenia przepisów prawa.

WYKAZ LOKALIZACJI I SPOSOBÓW UDOSTĘPNIANIA WW. INFORMACJI.

Lp.	Wersja	Lokalizacja
1.	elektroniczna	pspbilcza.szkolnastrona.pl
2.	elektroniczna	wiadomość e-mail
3.	papierowa	tablica ogłoszeń w siedzibie Szkoły
4.	papierowa	korespondencja listowna.