

Załącznik
do Zarządzenia nr 5/2018
Dyrektora Szkoły Podstawowej nr 2 im. J. Nojiego w Drezdenku
z dnia 9 kwietnia 2018 r.

Polityka Bezpieczeństwa ochrony i przetwarzania danych osobowych

oraz

Instrukcja zarządzania systemem informatycznym

w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

Obowiązuje od dnia 9 kwietnia 2018 r.

1. Wstęp.

1.1. Informacje ogólne.

1. Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Szkołę Podstawową nr 2 im. Józefa Nojiego w Drezdenku (dalej jako „Szkoła”) przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.
2. Wskazane dane osobowe będą przetwarzane przez Szkołę wyłącznie w celach określonych w niniejszym dokumencie.
3. Polityka obowiązuje wszystkich pracowników Szkoły oraz podmioty współpracujące lub świadczące na jej rzecz usługi na podstawie umów cywilnoprawnych, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.
4. Przetwarzanie danych osobowych w Szkole odbywa się w wersji papierowej i za pomocą systemów informatycznych.
5. Administratorem danych osobowych przetwarzanych w ww. sposób jest Szkoła Podstawowa nr 2 im. Józefa Nojiego w Drezdenku.
6. 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),
 - 2) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000 z późn. zm.)¹,
 - 3) 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.),
 - 4) 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.),
 - 5) 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.).

1.2. Zakres informacji objętych Polityką Bezpieczeństwa oraz zakres zastosowania.

1. Niniejsza Polityka Bezpieczeństwa określa zasady i procedury związane z przetwarzaniem danych osobowych. Jednocześnie wskazany dokument zawiera opis sposobów zabezpieczenia przetwarzanych danych osobowych.
2. Polityka Bezpieczeństwa zawiera informacje na temat:
 - 1) wykazu i zakresu przetwarzanych danych osobowych,
 - 2) programów stosowanych do przetwarzania ww. danych,
 - 3) wykazu budynków i pomieszczeń, w których przetwarzane są dane osobowe,
 - 4) sposobu przepływu danych pomiędzy poszczególnymi systemami,

¹ Zarządzenie nr 38/2020 Dyrektora Szkoła Podstawowa nr 2 im. J. Nojiego w Drezdenku z dnia 31 grudnia 2020 r.

- 5) środków technicznych i organizacyjnych wykorzystywanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
- 6) sposobu zarządzania systemem informatycznym zawierającym dane osobowe,
- 7) procedur postępowania w przypadku naruszenia postanowień i zasad ww. Polityki Bezpieczeństwa.

1.3. Wyjaśnienie terminów używanych w dokumencie Polityki Bezpieczeństwa:

- 1) Administrator Danych Osobowych – Szkoła Podstawowa nr 2 im. Józefa Nojiego w Drezdenku, plac Wolności 8, 66-530 Drezdenko,
- 2) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której dane są przetwarzane przez Szkołę,
- 3) Uczeń – należy przez to rozumieć osobę, która realizuje obowiązek szkolny w ramach jednostki administracyjnej jaką jest Administrator Danych Osobowych,
- 4) Identyfikator – należy przez to rozumieć elektroniczne, indywidualne oznaczenie pracownika w systemie informatycznym tzw. login,
- 5) Pracownik – należy przez to rozumieć osobę zatrudnioną przez Szkołę w formie umowy o pracę lub świadczącą na jej rzecz usługi na podstawie umów cywilnoprawnych,
- 6) Użytkownik systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Szkoły, Użytkownikiem systemu może być Pracownik,
- 6) Ustawa – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
- 7) 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),
- 8) Przetwarzanie danych – jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
- 9) Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

2. Osoby odpowiedzialne za ochronę danych osobowych.

2.1. Informacje ogólne.

1. Do kręgu osób odpowiedzialnych za przetwarzanie i ochronę danych osobowych Szkole należy zaliczyć:
 - 1) Administratora Danych Osobowych,
 - 2) Inspektora Ochrony Danych,
 - 3) Administratora Systemów Informatycznych (tylko i wyłącznie w przypadku powołania),
 - 4) osoby wykonujące pracę, bądź świadczące usługi cywilnoprawne na rzecz Szkoły, które uzyskały pisemne upoważnienie do przetwarzania danych osobowych.
2. Wskazane podmioty mają stały i regularny dostęp do danych osobowych, przetwarzając je oraz uniemożliwiając dostęp do nich osobom nieuprawnionym.

2.2. Administrator Danych Osobowych.

1. Administratorem Danych Osobowych jest Szkoła Podstawowa nr 2 im. Józefa Nojiego w Drezdenku. Administrator Danych Osobowych decyduje o celach i środkach przetwarzania danych osobowych.
2. 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 prawa 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) powoływanie Inspektora Ochrony Danych;
 - 7) powierzanie podmiotom trzecim przetwarzania danych osobowych na podstawie pisemnych umów.

2.3. Inspektor Ochrony Danych.

1. 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.:
 - 1) administratorem danych jest organ lub podmiot publiczny,
 - 2) główna działalność administratora polega na operacjach przetwarzania wymagających regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
 - 3) główna działalność administratora polega na przetwarzaniu na dużą skalę wrażliwych danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.
2. Do uprawnień i obowiązków Inspektora Ochrony Danych 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,
 - 4) informowanie Administratora Danych Osobowych oraz Pracowników o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz przepisów 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) przeprowadzanie szkoleń dla Pracowników z zakresu ochrony danych osobowych,
 - 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 (Załącznik nr 5 do Polityki Bezpieczeństwa) 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.
3. 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.

1. Wyznaczenie Administratora Systemów Informatycznych nie jest obowiązkiem, ale prawem Administratora Danych Osobowych. Decyzja o jego wyznaczeniu należy do Administratora Danych Osobowych.
2. 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.

2.5. Osoby upoważnione do przetwarzania danych osobowych – Użytkownicy systemu.

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych.
2. Osoba, która uzyskała upoważnienie do przetwarzania danych osobowych tj. Użytkownik systemu zobowiązana jest do ich ochrony w sposób zgodny z przepisami Rozporządzenia, Ustawy, rozporządzeń wymienionych w pkt. 1.1. niniejszego dokumentu, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.
3. 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.
4. Upoważnienie udzielane jest w formie pisemnej, przez Administratora Danych Osobowych. Upoważnienie sporządzane jest wg wzorów stanowiących Załączniki nr 4a i 4b 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.

1. Administrator Danych Osobowych jest zobowiązany do prowadzenia rejestru Użytkowników systemu i ich uprawnień w systemie informatycznym.
2. 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.

2.7. Odpowiedzialność Użytkowników systemu.

1. Użytkownik systemu zobowiązany jest do zachowania przetwarzanych danych w poufności oraz dołożenia wszelkich starań, aby te dane nie zostały przekazane osobom nieuprawnionym.
2. Użytkownik systemu ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
3. 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.
4. Wszelkie przekroczenia lub jakiegokolwiek próby przekroczenia przyznanych uprawnień, traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
5. W uzasadnionych sytuacjach Administrator Danych Osobowych może odebrać uprawnienia Użytkownikowi systemu z podaniem daty oraz przyczyny odebrania uprawnień.
6. 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.

3. Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych.

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

3.1. Upoważnienie do przetwarzania danych osobowych.

1. Upoważnienie do przetwarzania danych osobowych, którego wzory stanowią Załączniki nr 4a i 4b do Polityki Bezpieczeństwa jest dokumentem dającym określonym osobom prawo do przetwarzania ściśle określonych danych osobowych.
2. Upoważnienia do przetwarzania danych osobowych są nadawane przez Administratora Danych Osobowych.
3. Upoważnienie nadawane jest wyłącznie w formie pisemnej.
4. W upoważnieniu dokładnie określony jest zbiór danych osobowych, które Użytkownik systemu będzie mógł przetwarzać, jak również cel wskazanego przetwarzania.
5. 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.

3.2. Umowy powierzenia przetwarzania danych osobowych.

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych podmiotom trzecim na podstawie pisemnej umowy.
2. Umowa, na podstawie której nastąpi przekazanie przetwarzania danych osobowych musi zawierać 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.
3. Ww. umowa musi być zawarta w formie pisemnej.

4. Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych.

1. Podmiotem odpowiedzialnym za przetwarzanie danych osobowych i ich bezpieczeństwo jest Administrator Danych Osobowych.
2. 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 ponosi 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. Obowiązuje go bezwzględny zakaz pozostawiania materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym,

- 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 bezwzględny zakaz wynoszenia 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.²

1. 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.
2. Mając na uwadze minimalizację skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości obowiązują następujące procedury:
 - 1) każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu Administratora Danych Osobowych lub Inspektora Ochrony Danych;
 - 2) kontakt do w/w osoby w przypadku incydentu: tel. 95 762 06 05;
 - 3) do typowych podatności bezpieczeństwa danych osobowych należą:
 - a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
 - b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
 - c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek);
 - 4) do typowych incydentów bezpieczeństwa danych osobowych należą:
 - a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
 - b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twarde dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),

² Zarządzenie nr 24/2021 Dyrektora Szkoły Podstawowej nr 2 im. J. Nojiego w Dreźnie z dnia 1 października 2021 roku

- c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania);
- 5) w przypadku stwierdzenia wystąpienia incydu, Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające w toku, którego:
 - a) ustala zakres i przyczyny incydu oraz jego ewentualne skutki,
 - b) inicjuje ewentualne działania dyscyplinarne,
 - c) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydu,
 - d) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia;
- 6) Administrator Danych Osobowych dokumentuje wszelkie powyższe naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (Załącznik nr 8 do Polityki Bezpieczeństwa);
- 7) zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych;
- 8) w przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – Administrator zgłasza je organowi nadzorcemu;
- 9) jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

6. Kontrola przetwarzania i stanu zabezpieczenia danych osobowych.

1. Nadzór i kontrolę nad ochroną przetwarzanych danych osobowych sprawuje Administrator Danych Osobowych.
2. Jeżeli został ustanowiony Inspektor Ochrony Danych przejmuje on ww. obowiązki w zakresie ochrony i nadzoru wskazanych danych osobowych.
3. 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.

7. Opis struktury zbiorów danych wraz z zawartością poszczególnych pól informacyjnych.

1. Dane osobowe przetwarzane są przez Szkołę w wersji elektronicznej oraz papierowej.
2. Dotyczą one uczniów i opiekunów prawnych uczniów, pracowników szkoły oraz osób współpracujących ze szkołą na podstawie umów cywilnoprawnych.
3. Wskazane zestawienie danych i ich opis wraz z zawartością poszczególnych pól informacyjnych stanowi Załącznik nr 1 do Polityki Bezpieczeństwa.
4. Rejestr czynności przetwarzania danych osobowych stanowi Załącznik nr 2 do Polityki Bezpieczeństwa

8. Obszar, w którym przetwarzane są dane osobowe.

1. Przetwarzanie danych osobowych odbywa się we wszystkich budynkach Szkoły.
2. Dane dotyczące sprawozdawczości finansowej oraz dokumentacja pracownicza przechowywane są w siedzibie Szkoły oraz budynkach organu prowadzącego, w szczególności Referatu Oświaty w Urzędzie Miejskim w Drezdenku³.
3. Szczegółowy wykaz i opis obszarów, w którym są przetwarzane dane osobowe, których administratorem jest Szkoła zostały ujęte w Załączniku nr 3 do Polityki Bezpieczeństwa.
4. Odnośnie ww. obszarów stosowane są następujące procedury postępowania i środki bezpieczeństwa.
5. 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 (Załącznik nr 6 do Polityki Bezpieczeństwa) oraz Administrator Danych Osobowych, a w przypadku powołania także, Inspektor Ochrony Danych i Administrator Systemów Informatycznych.
6. Zabrania się przebywania osób postronnych w strefach bezpośrednio związanych z przetwarzaniem danych osobowych (komputery, szafy z aktami) pod nieobecność Administratora Danych Osobowych, Inspektora Ochrony Danych lub Administratora Systemów Informatycznych lub upoważnionego Użytkownika systemu.

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

1. Szkoła stosuje zróżnicowany wachlarz środków technicznych i organizacyjnych mających zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.
2. Szczegółowe zestawienie wskazanych środków zawierają wykazy stanowiące Załączniki nr 3a i 3b do Polityki Bezpieczeństwa.

10. Obowiązek informacyjny w przedmiocie przetwarzania danych osobowych.

1. Szkoła wypełnia obowiązek informacyjny o zakresie, celu, miejscu i czasie przetwarzania znajdujących się w jej posiadaniu danych osobowych.
2. W ramach realizacji ww. obowiązku Szkoła podaje osobom, których dane osobowe są przetwarzane, następujące informacje:
 - 1) swoją tożsamość i dane kontaktowe,
 - 2) dane kontaktowe Inspektora Ochrony Danych,
 - 3) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
 - 4) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców,
 - 5) informacje o ewentualnym zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
 - 6) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
 - 7) 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,
 - 8) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

³ Zarządzenie nr 38/2020 Dyrektora Szkoła Podstawowa nr 2 im. J. Nojiego w Drezdenku z dnia 31 grudnia 2020 r.

- 9) informacje o prawie wniesienia skargi do organu nadzorczego,
 - 10) 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.
3. Wzór informacji dotyczącej danych przetwarzanych przez Szkołę stanowi Załącznik nr 7 do Polityki Bezpieczeństwa.
- 11. Procedura związana ze sprostowaniem, ograniczeniem i usuwaniem danych osobowych oraz sprzeciwem.**
1. Szkoła realizuje obowiązki związane ze sprostowaniem, ograniczeniem i usuwaniem danych osobowych.
 2. Dokonanie ww. czynności następuje na wniosek podmiotu, którego dane osobowe dotyczą po zgłoszeniu i pozytywnej weryfikacji jego żądania.
 3. 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 wniosek może zostać przesłany w formie elektronicznej (dokument w formacie PDF) lub pisemnej papierowej. W przypadku złożenia wniosku drogą elektroniczną, ww. żądanie winne być opatrzone elektronicznym podpisem kwalifikowanym. W przypadku wniosku złożonego w formie pisemnej papierowej pod rygorem nieważności z podpisem potwierdzonym przez Szkołę za okazaniem dowodu osobistego, paszportu lub notarialnego poświadczenia,⁴
 - 3) spełnienie żądań osoby je kierującej nastąpi wyłącznie w przypadkach przewidzianych w Rozporządzeniu, jeżeli nie zachodzą okoliczności uprawniające Szkołę do dalszego przetwarzania danych mimo zgłoszonych żądań,
 - 4) Szkoła udzieli odpowiedzi na wystosowane żądanie sprostowania, ograniczenia i usunięcia danych lub złożonego sprzeciwu bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca.⁵
 4. Szkoła ma obowiązek usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
 - 1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
 - 2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
 - 3) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
 - 4) osoba, której dane dotyczą, wnosi sprzeciw, a jej dane są przetwarzane na potrzeby marketingu bezpośredniego,
 - 5) dane osobowe były przetwarzane niezgodnie z prawem,

⁴ Zarządzenie nr 24/2021 Dyrektora Szkoły Podstawowej nr 2 im. J. Nojiego w Drezdenku z dnia 1 października 2021 roku

⁵ Zarządzenie nr 24/2021 Dyrektora Szkoły Podstawowej nr 2 im. J. Nojiego w Drezdenku z dnia 1 października 2021 roku

- 6) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie krajowym,
 - 7) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.
5. Szkoła nie ma obowiązku usunąć danych w zakresie w jakim ich przetwarzanie jest niezbędne m.in.:
- 1) do korzystania z prawa do wolności wypowiedzi i informacji,
 - 2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa krajowego,
 - 3) do ustalenia, dochodzenia lub obrony roszczeń.
6. Szkoła ma obowiązek ograniczyć przetwarzanie danych osobowych, co należy rozumieć jako zawieszenie przetwarzania, jeżeli:
- 1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych,
 - 2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
 - 3) Szkoła nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
 - 4) 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.

12. 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.

1. Wprowadza się następujące zasady zabezpieczania sprzętu informatycznego, danych i oprogramowania:
 - 1) 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. Pomieszczenia, w których znajduje się sprzęt komputerowy służący do przetwarzania danych osobowych, jak również szafy z aktami zawierającymi dane osobowe znajdują się w budynkach chronionych systemem alarmowym. Budynki, w których znajdują się pomieszczenia zamykane są przez ostatnią osobę go opuszczającą;
 - 2) pracowników obowiązuje bezwzględny zakaz wnoszenia płyt lub innych nośników z oprogramowaniem lub innymi danymi poza teren siedziby jednostki, chyba że zgodę na taką czynność wyrazi Administrator Danych Osobowych;
 - 3) 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 komputera przenośnego;

- 4) 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;
- 5) na stanowiskach pracy, na których przetwarzane są dane osobowe, ekrany monitorów powinny być ustawione w sposób uniemożliwiający osobom trzecim wgląd w wyświetlane informacje;
- 6) 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.

13.2. Procedura rozpoczęcia i zakończenia pracy.

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

- 1) przy wejściu do systemu przetwarzającego dane osobowe wprowadza się identyfikator oraz hasło dostępu,
- 2) 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 powinny 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,
- 2) Użytkownicy systemu są odpowiedzialni za niedostępianie 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:

Naprawy sprzętu komputerowego użytkowanego w systemie może dokonywać jedynie wyspecjalizowany podmiot świadczący usługi 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 usługi 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.

13. Wydruki.

Odnosnie zabezpieczenia papierowej wersji danych osobowych wprowadza się następujące zasady:

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

Załącznik nr 1
do Polityki bezpieczeństwa ochrony i przetwarzania danych osobowych
w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

Rejestr zbiorów danych osobowych przetwarzanych w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

Lp.	Nazwa zbioru	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane w zbiorze	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego	Wersja papierowa
1.	Rekrutacja - Zgłoszenie lub wnioski o przyjęcie do szkoły/oddziału przedszkolnego – informacje dot. kandydata przyjmowanego do szkoły/oddziału przedszkolnego „0”	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe ze zm. oraz rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji ze zm.	Obowiązki wynikające z przepisów prawa	1. Kandydaci 2. Rodzice/opiekunowie prawni kandydatów 3. Członkowie rodziny kandydata	Nazwiska i imiona, data i miejsce urodzenia, adres zamieszkania/zameldowania, pesel, telefon, e-mail	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
2.	Dziennik lekcyjny (w tym elektroniczny) - Dokumentacja przebiegu nauczania w danym roku szkolnym	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe ze zm. oraz rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów	Nazwiska i imiona, data i miejsce urodzenia, adres zamieszkania/zameldowania, telefon	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
3.	Dziennik zajęć dodatkowych (w tym zajęć specjalistycznych, nauczania indywidualnego etc.)	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe ze zm. oraz rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów	Nazwiska i imiona, data i miejsce urodzenia, adres zamieszkania/zameldowania, telefon	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak

----- TEKST UJEDNOLICONY -----

Lp.	Nazwa zbioru	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane w zbiorze	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego	Wersja papierowa
4.	Arkusze Ocen - dokumentacja wyników nauczania ucznia w poszczególnych latach	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe ze zm. oraz rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji ze zm..	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów	Nazwiska i imiona, data i miejsce urodzenia, adres zamieszkania, pesel, nr księgi uczniów, przebieg nauki, wyniki nauki	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
5.	Protokoły Rady Pedagogicznej	brak	Rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów 3. Pracownicy pedagogiczni	Nazwiska i imiona, data urodzenia, przebieg nauki, wyniki nauki, opinie i orzeczenia PPP	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
6.	Lista uczestników wycieczek	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 8 listopada 2001 r. w sprawie warunków i sposobu organizowania przez publiczne szkoły i placówki krajoznawstwa i turystyki ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów 3. Nauczyciele 4. Opiekunowie	Nazwisko i imię, data i miejsce urodzenia, adres zamieszkania, PESEL, telefon opiekuna	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
7.	Świadectwa szkolne	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Rozporządzenie Ministra Edukacji Narodowej z dnia 28 maja 2010 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie	Nazwisko i imiona, data i miejsce urodzenia, pesel, wyniki nauki	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
8.	Ewidencja świadectw szkolnych	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Ustawa z dnia 7 września 1991 r. o systemie oświaty ze zm. oraz rozporządzenie Ministra Edukacji Narodowej z dnia 28 maja 2010 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie	Nazwisko i imię, PESEL, nr księgi uczniów	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
9.	Ewidencja legitymacji szkolnych	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Rozporządzenie Ministra Edukacji Narodowej z dnia 28 maja 2010 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie	Nazwisko i imię, PESEL	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak

----- TEKST UJEDNOLICONY -----

Lp.	Nazwa zbioru	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane w zbiorze	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego	Wersja papierowa
10.	Dokumentacja PPP - Pomoc psychologiczno-pedagogiczna	System Informacji Oświatowej (SIO) Wolters Kluwer Polska z siedzibą w Warszawie przy ul. Przyokopowa 33	Rozporządzenie Ministra Edukacji Narodowej z dnia 9 sierpnia 2017 r. w sprawie zasad organizacji i udzielania pomocy psychologiczno-pedagogicznej w publicznych przedszkolach, szkołach i placówkach ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów	Nazwisko i imię, PESEL, data i miejsce urodzenia, adres zamieszkania, informacja o specjalnych potrzebach	Dane zbierane od osób, których dane osobowe dotyczą	Organ prowadzący	Nie dotyczy	Tak
11.	Oświadczenia o nauce religii/etyki i WDŻ	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Ustawa z dnia 7 września 1991 r. o systemie oświaty ze zm., rozporządzenia MEN z dnia 14 kwietnia 1992 r. w sprawie warunków i sposobu organizowania nauki religii w publicznych przedszkolach i szkołach ze zm. oraz rozporządzenia MEN z dnia 12 sierpnia 1999 r. w sprawie sposobu nauczania szkolnego oraz zakresu treści dotyczących wiedzy o życiu seksualnym człowieka, o zasadach świadomego i odpowiedzialnego rodzicielstwa, o wartości rodziny, życia w fazie prenatalnej oraz metodach i środkach świadomej prokreacji zawartych w podstawie programowej kształcenia ogólnego	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów	Nazwisko i imię, przynależność wyznaniowa	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
12.	Świetlica „0-3” - informacje o uczniach, zgłoszonych do świetlicy szkolnej	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Ustawa z dnia 7 września 1991 r. o systemie oświaty ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów 3. Osoby upoważnione do odbioru ucznia	Nazwisko i imiona, adres zamieszkania, nr i seria dowodu osobistego, telefon	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
13.	Monitoring - system monitoringu CCTV	brak	Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów 3. Osoby upoważnione do odbioru ucznia 4. Kontrahenci 5. Osoby przebywające na terenie lub wokół Szkoły	Wizerunek	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak

----- TEKST UJEDNOLICONY -----

Lp.	Nazwa zbioru	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane w zbiorze	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego	Wersja papierowa
14.	Dane fakturowe - Kontrahenci, umowy cywilno-prawne	Wolters Kluwer Polska z siedzibą w Warszawie przy ul. Przyokopowa 33	Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny ze zm., ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych ze zm. oraz ustawa z dnia 29 września 1994 r. o rachunkowości ze zm.	Obowiązki wynikające z przepisów prawa	1. Kontrahenci (osoby fizyczne)	Nazwisko i imiona, adres zamieszkania/adres prowadzenia działalności gospodarczej, NIP, telefon, e-mail	Dane zbierane od osób, których dane osobowe dotyczą	Organ prowadzący	Nie dotyczy	Tak
15.	Dane OKE - informacje o uczniach, zgłoszonych do egzaminu zewnętrznego	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193 System Informacji Oświatowej (SIO)	Rozporządzenie Ministra Edukacji Narodowej z dnia 21 grudnia 2016 r. w sprawie szczegółowych warunków i sposobu przeprowadzania egzaminu gimnazjalnego i egzaminu maturalnego ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie	Nazwisko i imiona, PESEL, informacja o specjalnych potrzebach, wyniki nauki	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
16.	Dziennik Pedagoga - Dziennik zawiera informacje o uczniach zakwalifikowanych do różnych form pomocy	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe ze zm. oraz rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów	Nazwiska i imiona, informacje o specjalnych potrzebach oraz o kontaktach z innymi osobami/institucjami	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
17.	Dokumentacja Pedagoga - Dokumentacja badań i czynności uzupełniających prowadzonych przez pedagoga	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe ze zm. oraz rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów	Dane niezbędne do dokumentowania przebiegu terapii, nazwiska i imiona, data urodzenia, adres zamieszkania/zameldowania, opinia lub orzeczenie PPP	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
18.	Biblioteka	VULCAN sp. z o.o z siedzibą we Wrocławiu przy ul. Wołowskiej 6	Ustawa z dnia 7 września 1991 r. o systemie oświaty ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów	Nazwisko i imię, adres zamieszkania, dane o wypożyczeniach	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak

----- TEKST UJEDNOLICONY -----

Lp.	Nazwa zbioru	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane w zbiorze	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego	Wersja papierowa
19.	Akta osobowe - Zbiór zatrudnionych pracowników	System Informacji Oświatowej (SIO) Wolters Kluwer Polska z siedzibą w Warszawie przy ul. Przyokopowa 33	Ustawa z dnia 26 stycznia 1982 r. Karta Nauczyciela ze zm. oraz ustawa z dnia 26 czerwca 1974 r. Kodeks pracy ze zm.	Obowiązki wynikające z przepisów prawa	1. Pracownicy 2. Członkowie rodziny pracowników	Nazwisko i imiona, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, seria i nr dowodu osobistego, adres zamieszkania, PESEL, wykształcenie, przebieg dotychczasowego zatrudnienia, informacja o karalności	Dane zbierane od osób, których dane osobowe dotyczą	Organ prowadzący	Nie dotyczy	Tak
20.	Dokumentacja wypadków uczniów - Informacje o wypadkach uczniów	System Informacji Oświatowej (SIO)	Rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002 r. ze zm. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie	Nazwisko i imiona, informacja o wypadku ucznia	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
21.	Dokumentacja wypadków pracowników - Informacje o wypadkach pracowników	brak	Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy ze zm.	Obowiązki wynikające z przepisów prawa	1. Pracownicy	Nazwisko i imiona, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, PESEL, seria i nr dowodu osobistego, informacja o wypadku	Dane zbierane od osób, których dane osobowe dotyczą	Organ prowadzący	Nie dotyczy	Tak
22.	Awans zawodowy	Wolters Kluwer Polska z siedzibą w Warszawie przy ul. Przyokopowa 33	Ustawa z dnia 26 stycznia 1982 r. Karta Nauczyciela ze zm. oraz rozporządzenie Ministra Edukacji Narodowej z dnia 1 marca 2013 r. w sprawie uzyskiwania stopni awansu zawodowego przez nauczycieli ze zm.	Obowiązki wynikające z przepisów prawa	1. Pracownicy	Nazwisko i imiona, nazwisko rodowe, data urodzenia, adres zamieszkania, przebieg zatrudnienia, wykształcenie, zapytanie o karalność	Dane zbierane od osób, których dane osobowe dotyczą	Organ prowadzący	Nie dotyczy	Tak
23.	Rejestr Korespondencji	brak	Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych	Obowiązki wynikające z przepisów prawa	1. Nadawcy korespondencji 2. Odbiorcy korespondencji	Nazwisko i imię, adres, e-mail	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak

----- TEKST UJEDNOLICONY -----

Lp.	Nazwa zbioru	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane w zbiorze	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego	Wersja papierowa
24.	Zbiór danych osobowych osób fizycznych uczestniczących w postępowaniach w trybie zamówień publicznych	brak	Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych ze zm.	Obowiązki wynikające z przepisów prawa	1. Osoby fizyczne uczestniczące w postępowaniach w trybie zamówień publicznych	Nazwisko i imię, adres, telefon, e-mail	Dane zbierane od osób, których dane osobowe dotyczą	Organ prowadzący	Nie dotyczy	Tak
25.	Księga Ewidencji Uczniów - Zbiór danych o uczniach uczących się w Szkole	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193 System Informacji Oświatowej (SIO)	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe ze zm. oraz rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji ze zm.	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów	Nazwiska i imiona, data i miejsce urodzenia, adres zamieszkania/zameldowania, pesel, przyjęcie do szkoły: data, klasa, semestr, obwód szkolny, profil. Wypisanie ze szkoły: data, klasa, powody. Data: wydania dokumentów, ukończenia szkoły.	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
26.	Księga ewidencji dzieci podlegających obowiązkowi szkolnemu i rocznego przygotowania przedszkolnego	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe ze zm., rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji ze zm.	Obowiązki wynikające z przepisów prawa	1. Dzieci 2. Rodzice/opiekunowie prawni dzieci	Nazwisko i imiona, pesel, data i miejsce urodzenia, adres zamieszkania	Dane zbierane od osób, których dane osobowe dotyczą oraz z Urzędu Miejskiego w Drezdenku	Organ prowadzący	Nie dotyczy	Tak
27.	Absolwenci - informacje o uczniach, którzy ukończyli Szkołę	Librus sp. z o.o. sp. k. z siedzibą w Katowicach przy al. Korfantego 193 System Informacji Oświatowej (SIO)	Rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji ze zm.	Obowiązki wynikające z przepisów prawa	1. Absolwenci Szkoły	Nazwisko i imiona, PESEL, adres zamieszkania	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
28.	Rekrutacja pracowników - dane osobowe kandydatów na pracowników Szkoły	brak	Ustawa z dnia 26 stycznia 1982 r. Karta Nauczyciela ze zm. oraz ustawa z dnia 26 czerwca 1974 r. Kodeks pracy ze zm.	Obowiązki wynikające z przepisów prawa	1. Kandydaci ubiegający się o pracę w Szkole	Nazwisko i imię, adres zamieszkania, telefon, e-mail, wykształcenie, przebieg dotychczasowego zatrudnienia	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak

TEKST UJEDNOLICONY

Lp.	Nazwa zbioru	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane w zbiorze	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego	Wersja papierowa
29.	Składnica akt	brak	Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach ze zm., rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych ze zm., Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych	Obowiązki wynikające z przepisów prawa	1. Uczniowie 2. Rodzice/opiekunowie prawni uczniów 3. (Byli) pracownicy 4. Członkowie rodzin (byłych) pracowników 5. Kontrahenci 6. Nadawcy i odbiorcy korespondencji 7. Osoby uczestniczące w postępowaniach w trybie zam. publ. 8. Kandydaci, ich rodzice/opiekunowie prawni oraz członkowie rodzin 9. Dzieci oraz ich rodzice/opiekunowie prawni 10. Studenci, praktykanci 11. Osoby odbywające staż/prace interwencyjne/praktyki zawodowe 12. Kandydaci ubiegający się o pracę w Szkole 13. Absolwenci Szkoły 14. Osoby upoważnione do odbioru ucznia	Nazwiska i imiona, data i miejsce urodzenia, adres zamieszkania/zameldowania, pesel, telefon, e-mail, dane dot. przyjęcia do szkoły, dane dot. wypisania ze szkoły, nr księgi uczniów, przebieg nauki, wyniki nauki, opinie i orzeczenia PPP, dane o wypożyczeniach, informacja o wypadku ucznia, przynależność wyznaniowa, informacje o specjalnych potrzebach oraz o kontaktach z innym i osobami/instytucjami, dane niezbędne do dokumentowania przebiegu terapii, nazwisko rodowe, imiona rodziców, seria i nr dowodu osobistego, wykształcenie, przebieg dotychczasowego zatrudnienia, informacja o karalności, sytuacja materialna, stan zdrowia, informacja o wypadku, adres prowadzenia działalności gospodarczej, NIP	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak

----- TEKST UJEDNOLICONY -----

Lp.	Nazwa zbioru	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane w zbiorze	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego	Wersja papierowa
30.	Studenci, praktykanci	brak	Na podstawie porozumienia pomiędzy uczelnią a Szkołą	Obowiązki wynikające z przepisów prawa	1. Studenci, praktykanci	Nazwisko i imię, adres zamieszkania, data i miejsce urodzenia, telefon	Dane zbierane od osób, których dane osobowe dotyczą	Nie dotyczy	Nie dotyczy	Tak
31.	Stażyści, pracownicy interwencyjni, osoby odbywające praktyki zawodowe	brak	Na podstawie porozumienia pomiędzy urzędem pracy a Szkołą	Obowiązki wynikające z przepisów prawa	1. Osoby odbywające staż/prace interwencyjne/praktyk i zawodowe	Nazwisko i imię, adres zamieszkania, data i miejsce urodzenia, telefon	Dane zbierane od osób, których dane osobowe dotyczą oraz z Powiatowego Urzędu Pracy	Nie dotyczy	Nie dotyczy	Tak
32.	ZFŚS - Świadczenia dla pracowników Dane o emerytach i rencistach, byłych pracownikach Szkoły	brak	Ustawa z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych ze zm.	Obowiązki wynikające z przepisów prawa	1. Pracownicy 2. Byli pracownicy 3. Członkowie rodziny (byłych) pracowników	Nazwisko i imiona, adres zamieszkania, sytuacja materialna, stan zdrowia	Dane zbierane od osób, których dane osobowe dotyczą	Organ prowadzący	Nie dotyczy	Tak

Załącznik nr 2
do Polityki bezpieczeństwa ochrony i przetwarzania danych osobowych
w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

Rejestr czynności przetwarzania danych osobowych w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

**Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar,
w którym przetwarzane są dane osobowe⁶**

Siedziba Szkoły znajduje się w miejscowości Drezdenko przy placu Wolności 8. Cała dokumentacja, w której przetwarzane są dane osobowe, przechowywana jest w budynkach Szkoły Podstawowej oraz budynkach organu prowadzącego (Drezdenko, Warszawska 1).

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

Dane w wersji elektronicznej przetwarzane są na komputerach stacjonarnych i przenośnych.

Dane w wersji papierowej przechowywane są w szafach zamykanych na klucz, znajdujących się w budynkach Szkoły, w pomieszczeniach zamykanych na klucz. Budynki są monitorowane, część z nich wyposażona jest w alarm, teren szkoły jest ogrodzony a bramy wjazdowe zamykane na klucz.

Lp.	Dokładny adres	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
1.	Szkoła Podstawowa nr 2 im. J. Nojiego w Drezdenku (66-530 Drezdenko, plac Wolności 8)	sekretariat	A1	drzwi zamykane na klucz	kluczami dysponuje dyrektor i wicedyrektor, pracownicy sekretariatu, sprzątaczką
		gabinet dyrektora	A1	drzwi zamykane na klucz	kluczami dysponuje dyrektor i wicedyrektor, pracownicy sekretariatu, sprzątaczką
		gabinet pedagoga	A11	drzwi zamykane na klucz	kluczami dysponuje pedagog, sprzątaczką
		gabinet intendenta	D3,D4	drzwi zamykane na klucz	kluczami dysponuje intendent
		pokój nauczycielski	A2	drzwi zamykane na klucz	klucze dostępne u dyrektora szkoły
		składnica akt	A11	drzwi zamykane na klucz	kluczami dysponuje dyrektor i pracownicy sekretariatu
		biblioteka	C3	drzwi zamykane na klucz	kluczami dysponuje dyrektor i nauczyciel bibliotekarz
		sale lekcyjne	A4,A5,A6,A7,A8,A9,A10, B1,B2,B3,B4,B5,B6,C1, C2,C4,C5,C6,C7,D1,D2	drzwi zamykane na klucz	klucze dostępne w pokoju nauczycielskim
2.	Urząd Miejski w Drezdenku (66-530 Drezdenko, ul. Warszawska 1)	księgowość, kadry	Pokój: 5, 115, 116, 117, 118, 120	drzwi zamykane na klucz	Referat Oświaty, sekretariat, biuro obsługi klienta

Kopie ww. kluczy znajdują się w sekretariacie Szkoły.

⁶ Zarządzenie nr 38/2020 Dyrektora Szkoła Podstawowa nr 2 im. J. Nojiego w Drezdenku z dnia 31 grudnia 2020 r.

Załącznik nr 3a
do Polityki bezpieczeństwa ochrony i przetwarzania danych osobowych
w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

**Środki ochrony technicznej i fizycznej niezbędne dla zapewnienia
poufności, integralności i rozliczalności przetwarzanych danych osobowych**

L.p.	Środek ochrony technicznej i fizycznej
1.	Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych są pod nadzorem Pracowników.
2.	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej na klucz szafie lub w pomieszczeniu zamykanym na klucz.
3.	Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej na klucz szafie lub pomieszczeniu zamykanym na klucz.
4.	Pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojących gaśnic.
5.	Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
6.	Zastosowano system monitoringu.
7.	Poczta elektroniczna e-mail łączy się przez SSL (połączenie zabezpieczone).
8.	Naprawa komputera następuje na miejscu, dane z dysku twardego takiego komputera kopiowane są na drugi komputer z danego działu.
9.	Istnieje możliwość skorzystania ze wsparcia technicznego firmy zewnętrznej tworzącej oprogramowanie.
10.	W przypadku awarii komputera, przed oddaniem go do naprawy, dysk jest formatowany celem pozbawienia go danych osobowych.
11.	Urządzenia przenoszące dane na zewnątrz oraz cały sprzęt komputerowy jest zewidencjonowany.
12.	W przypadku zgubienia lub uszkodzenia urządzenia przenoszącego dane jest to zgłaszane niezwłocznie Administratorowi Danych Osobowych.

Załącznik nr 3b
do Polityki bezpieczeństwa ochrony i przetwarzania danych osobowych
w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

**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 Osobowych.
2.	Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
3.	Opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych.
4.	Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
5.	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
6.	Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
7.	Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy.
8.	Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, działając w imieniu Szkoły Podstawowej nr 2 im. Józefa Nojiego w Drezdenku, **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 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 zobowiązuje się do ich stosowania.

Jestem świadoma/y 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

Załącznik nr 4b
do Polityki bezpieczeństwa ochrony i przetwarzania danych osobowych
w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH (dla osób zatrudnionych na podstawie innej umowy niż umowa o pracę)

Niniejszym, działając w imieniu Szkoły Podstawowej nr 2 im. Józefa Nojiego w Drezdenku, **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 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 zobowiązuje się do ich stosowania.

Jestem świadoma/y 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

Załącznik nr 5
do Polityki bezpieczeństwa ochrony i przetwarzania danych osobowych
w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

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.				
15.				

Załącznik nr 6
do Polityki bezpieczeństwa ochrony i przetwarzania danych osobowych
w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

**Wykaz podmiotów, którym Administrator Danych Osobowych
powierzył przetwarzanie danych osobowych**

Podmioty, którym Administrator Danych Osobowych powierzył przetwarzanie danych osobowych	Adres / lokalizacja (NIP, REGON)	Uwagi

Załącznik nr 7
do Polityki bezpieczeństwa ochrony i przetwarzania danych osobowych
w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

Wzór informacji dotyczących przetwarzania danych osobowych wraz wykazem lokalizacji i sposobów jej udostępniania

Niniejszym zgodnie z art. 13 ust. 1 i ust. 2 *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)* przekazujemy Państwu wymagane prawem informacje.

ADMINISTRATOR DANYCH OSOBOWYCH

Administratorem danych osobowych uczniów Szkoły Podstawowej nr 2 im. J. Nojiego w Drezdenku jest Szkoła Podstawowa nr 2 im. J. Nojiego w Drezdenku:

adres: plac Wolności 8, 66-530 Drezdenko
telefon: 95 762 06 05
e-mail: sp2drezdenko@gmail.com

INSPEKTOR OCHRONY DANYCH

Nadzór nad prawidłowym przetwarzaniem danych osobowych w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku pełni Inspektor Ochrony Danych (IOD). Kontakt do Inspektora Ochrony Danych (IOD):
e-mail: iod.sp2drezdenko@gmail.com

CEL PRZETWARZANIA DANYCH OSOBOWYCH UCZNIÓW

Dane osobowe uczniów (w tym ich rodziców/opiekunów prawnych) są przetwarzane w celu:

- 1) wypełnienia obowiązków Administratora wynikających z przepisów prawa (Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe - Dz.U. 2017 poz. 59 ze zm.; Ustawa z dnia 7 września 1991 r. o systemie oświaty - Dz.U. 2017 poz. 2198 ze zm.; Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej - Dz.U. 2017 poz. 2159 ze zm.) na podstawie art. 6 ust. 1 pkt c *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* (tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze),
- 2) zapewnienia bezpieczeństwa uczniów oraz dla ochrony mienia i zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Szkołę Podstawową nr 2 im. J. Nojiego w Drezdenku na szkodę, poprzez zastosowanie środków technicznych umożliwiających rejestrację obrazu (monitoring wizyjny) - zgodnie z art. 108a Ustawy z dnia 14 grudnia 2016 r. prawo oświatowe.
- 3) realizacji celów związanych z promocją działań Szkoły Podstawowej nr 2 im. J. Nojiego w Drezdenku poprzez udostępnianie, np. na oficjalnej stronie internetowej lub szkolnym profilu na Facebooku – informacji o sukcesach konkretnych uczniów, informacji o wydarzeniach, przedsięwzięciach, w których uczniowie brali udział (np. konkursy, zawody sportowe), w tym także wizerunków uczniów – wyłącznie w przypadkach, gdy rodzice, opiekunowie wyrazili zgodę na taką formę przetwarzania.

KOMU DANE BĘDĄ UDOSTĘPNIANE

Dostęp do danych osobowych uczniów wewnątrz struktury organizacyjnej Szkoły Podstawowej nr 2 im. J. Nojiego w Drezdenku będą mieć wyłącznie upoważnieni pracownicy i tylko w zakresie niezbędnym do realizacji obowiązków zawodowych.

Odbiorcami danych osobowych będą organy publiczne, instytucje i podmioty trzecie uprawnione do żądania dostępu lub otrzymania danych osobowych na podstawie przepisów prawa (np. Kuratorium Oświaty, policja, Ośrodek Pomocy Społecznej), a także podmioty, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. dostawcą oprogramowania, zewnętrznym audytorem).

Dane przetwarzane w celach związanych z promocją jednostki będą udostępniane, rozpowszechniane poprzez umieszczenie np. na tablicach informacyjnych, szkolnej gazetce, oficjalnych szkolnych stronach internetowych, szkolnym profilu na Facebooku.

----- TEKST UJEDNOLICONY -----

OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

Dane osobowe uczniów będą przechowywane przez Szkołę Podstawową nr 2 im. J. Nojiego w Drezdenku przez okres niezbędny do realizacji wynikających z Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. 2018 poz. 217 ze zm.) celów archiwizacji. Dane przetwarzane na podstawie zgody będą przechowywane do momentu wycofania zgody.

KATEGORIE PRZETWARZANYCH DANYCH OSOBOWYCH UCZNIÓW

W związku z nauką w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku, Szkoła może przetwarzać w szczególności następujące dane uczniów:

Lp.	Kategorie danych	Podstawa prawna
1.	dane identyfikacyjne ucznia, takie jak imię, nazwisko, nr PESEL, data urodzenia, adres zamieszkania i zameldowania, itp.	Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe; Ustawa z dnia 7 września 1991 r. o systemie oświaty;
2.	informacje na temat potrzeb edukacyjnych dziecka (np. opinie, orzeczenia poradni psychologiczno-pedagogicznych)	Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej
3.	dane identyfikacyjne rodziców, opiekunów ucznia, takie jak imiona i nazwiska, adres zamieszkania, numery telefonów, adres e-mail	Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe - Dz.U. 2017 poz. 59 ze zm.; Ustawa z dnia 7 września 1991 r. o systemie oświaty - Dz.U. 2017 poz. 2198 ze zm.
4.	informacje niezbędne do zapewnienia dziecku właściwej opieki, w czasie zajęć organizowanych przez Szkołę	
5.	Informacje nt. sytuacji wychowawczej ucznia	
6.	Informacje dotyczące frekwencji ucznia na zajęciach szkolnych, informacje o wynikach edukacyjnych dziecka, jego zachowaniu, informacje nt. jego rozwoju	
7.	Informacje o wynikach ucznia w konkursach, zawodach międzyszkolnych i innych wydarzeniach	art. 108a Ustawy z dnia 14 grudnia 2016 r. prawo oświatowe – Dz.U. 2017 poz. 59 ze zm.
8.	Wizerunek zarejestrowany poprzez instalację monitoringu wizyjnego w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku w związku z zapewnieniem bezpieczeństwa oraz dla ochrony mienia i zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić jednostkę na szkodę	
9.	Wizerunek ucznia utrwalony przy okazji prowadzenia dokumentacji fotograficznej i video szkolnych uroczystości, zawodów, innych wydarzeń	Zgoda wyrażona przez rodziców, opiekunów prawnych ucznia

PRAWO DOSTĘPU

Niniejszym informujemy, że posiadają Państwo prawo dostępu do treści danych swoich dzieci oraz prawo do ich sprostowania, a w przypadku przetwarzania danych na podstawie zgody, do ich usunięcia.

PRAWO DO SKARGI

Mają Państwo prawo wniesienia skargi do organu nadzorczego dot. ochrony danych osobowych, gdy uznają Państwo, iż przetwarzanie danych osobowych Państwa dziecka narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

KONSEKWENCJE NIEPODANIA DANYCH

Podanie danych osobowych opisanych w rubryce 1-8 ucznia jest wymogiem ustawowym. Są Państwo zobowiązani do ich podania, a konsekwencją ich niepodania będzie brak możliwości edukacji Państwa dziecka w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku.

Przetwarzanie danych opisanych w rubryce nr 9 zależy od dobrowolnej zgody rodziców, opiekunów prawnych naszych uczniów. Brak zgody w tym zakresie będzie skutkował pominięciem informacji dotyczących Państwa dziecka w podanych informacjach o sukcesach, wydarzeniach, w których brało ono udział.

Załącznik nr 8
do Polityki bezpieczeństwa ochrony i przetwarzania danych osobowych
w Szkole Podstawowej nr 2 im. J. Nojiego w Drezdenku

Zgłoszenie naruszenia ochrony danych osobowych

1. Typ zgłoszenia					
Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.					
Podaj swoją sygnaturę sprawy (opcjonalnie) (np. sygnatura w Twoim wewnętrznym rejestrze naruszeń) Kliknij tutaj, aby wprowadzić tekst.					
 Zgłoszenie kompletne/jednorazowe	 Zgłoszenie wstępne		 Zgłoszenie uzupełniające/zmieniające		
	Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę.		Podaj datę poprzedniego zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę. Podaj sygnaturę sprawy UODO Kliknij tutaj, aby wprowadzić datę.		
2. Podmiot zgłaszający					
2A. Dane administratora danych					
Pełna nazwa administratora Kliknij tutaj, aby wprowadzić tekst.					
REGON (opcjonalnie)	Podaj numer.	NIP (opcjonalnie)	Podaj numer.	KRS (opcjonalnie)	Podaj numer.
Sektor (opcjonalnie)	Dla sektora publicznego: Wybierz element.		Dla sektora prywatnego: Wybierz element.		
2B. Adres siedziby administratora danych					
Ulica	Kliknij tutaj, aby wprowadzić tekst.		Numer domu	Podaj numer	Numer lokalu Podaj numer
Miejscowość	Kliknij tutaj, aby wprowadzić tekst.		Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.	
Gmina	Kliknij tutaj, aby wprowadzić tekst.		Powiat	Kliknij tutaj, aby wprowadzić tekst.	
Województwo	Kliknij tutaj, aby wprowadzić tekst.		Państwo	Kliknij tutaj, aby wprowadzić tekst.	
2C. Osoby uprawnione do reprezentowania administratora					
1.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.	
(Aby dopisać kolejne osoby, należy po kliknięciu na powyższe pole kliknąć przycisk , który pojawi się po prawej stronie)					
2D. Pełnomocnik					
☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)					
Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo udzielone w formie elektronicznej (zgodnie z art. 33a KPA) oraz dowód uiszczenia opłaty skarbowej					

----- TEKST UJEDNOLICONY -----

2E. Inspektor ochrony danych

Imię i nazwisko Numer telefonu Adres e-mail

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

2F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie (np. podmiot przetwarzający, współadministrator, operator pocztowy itp.)

1.	Nazwa i dane kontaktowe	Rola
	Kliknij tutaj, aby wprowadzić tekst.	Kliknij tutaj, aby wprowadzić tekst.

(Aby dopisać kolejne podmioty, należy po kliknięciu na powyższe pole kliknąć przycisk , który pojawi się po prawej stronie)

3. Czas naruszenia

3A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia
Wskaż kiedy dowiedziałeś/aś się o naruszeniu.
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

3B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Data i czas zakończenia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

[Kliknij tutaj, aby wprowadzić tekst.](#)

4B. Na czym polegało naruszenie?

- | | |
|--|--|
| ☐ Zgubienie lub kradzież nośnika/urządzenia
☐ Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji
☐ Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy
☐ Nieuprawnione uzyskanie dostępu do informacji
☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń
☐ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych
☐ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing) | ☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie
☐ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora
☐ Niezamierzona publikacja
☐ Dane osobowe wystane do niewłaściwego odbiorcy
☐ Ujawnienie danych niewłaściwej osoby
☐ Ustne ujawnienie danych osobowych |
|--|--|

4C. Przyczyna naruszenia

- ☐ Wewnętrzne działanie niezamierzone
☐ Wewnętrzne działanie zamierzone
☐ Zewnętrzne działanie niezamierzone
☐ Zewnętrzne działanie zamierzone

4D. Charakter

- ☐ **Naruszenie poufności danych**
Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych
☐ **Naruszenie integralności danych**
Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania
☐ **Naruszenie dostępności danych**
Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

4E. Dzieci

- ☐ **Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.**
(opcjonalnie)

5. Liczba osób i wpisów

Przybliżona liczba osób, których mogło dotyczyć naruszenie

[Kliknij tutaj, aby wprowadzić tekst.](#)

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

[Kliknij tutaj, aby wprowadzić tekst.](#)

6. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

6A. Dane podstawowe

- | | |
|--|---|
| ☐ Nazwiska i imiona | ☐ Nazwa użytkownika i/lub hasło |
| ☐ Imiona rodziców | ☐ Dane dotyczące zarobków i/lub posiadanego majątku |
| ☐ Data urodzenia | ☐ Nazwisko rodowe matki |
| ☐ Numer rachunku bankowego | ☐ Seria i numer dowodu osobistego |
| ☐ Adres zamieszkania lub pobytu | ☐ Numer telefonu |
| ☐ Numer ewidencyjny PESEL | ☐ Wizerunek |
| ☐ Adres e-mail | ☐ Inne, wskaż jakie: <input type="text" value="Kliknij tutaj, aby wprowadzić tekst."/> |

6B. Dane szczególnej kategorii

- | | |
|---|---|
| ☐ Dane o pochodzeniu rasowym lub etnicznym | ☐ Dane dotyczące seksualności lub orientacji seksualnej |
| ☐ Dane o poglądach politycznych | ☐ Dane dotyczące zdrowia |
| ☐ Dane o przekonaniach religijnych lub światopoglądowych | ☐ Dane genetyczne |
| ☐ Dane o przynależności do związków zawodowych | ☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej |

6C. Dane, o których mowa w art. 10 RODO

- | | | |
|---|---|---|
| ☐ Dane dotyczące wyroków skazujących | ☐ Dane dotyczące czynów zabronionych | ☐ Inne <input type="text" value="Kliknij tutaj, aby wprowadzić tekst."/> |
|---|---|---|

7. Kategorie osób

- | | |
|---|--|
| ☐ Pracownicy | ☐ Klienci (obecni i potencjalni) |
| ☐ Użytkownicy | ☐ Klienci podmiotów publicznych |
| ☐ Subskrybenci | ☐ Pacjenci |
| ☐ Studenci | ☐ Dzieci |
| ☐ Uczniowie | ☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.) |
| ☐ Służby mundurowe (np. wojsko, policja) | |

Szczegółowy opis kategorii osób, których dotyczy naruszenie:

Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie

W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

8. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

- | | |
|--|---|
| ☐ Utrata kontroli nad własnymi danymi osobowymi | ☐ Strata finansowa |
| ☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO | ☐ Naruszenie dobrego imienia |
| ☐ Ograniczenie możliwości realizowania praw | ☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową |
| ☐ Dyskryminacja | ☐ Nieuprawnione odwrócenie pseudonimizacji |
| ☐ Kradzież lub sfałszowanie tożsamości | ☐ Inne <small>Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:</small> |
-

8B. Ryzyko naruszenia praw i wolności osób fizycznych

- | | | |
|---|-------------------------------|-------------------------------|
| ☒ Niskie | ☐ Średnie | ☐ Wysokie |
|---|-------------------------------|-------------------------------|

9. Środki bezpieczeństwa i środki zaradcze

9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

Kliknij tutaj, aby wprowadzić tekst.

9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia

Kliknij tutaj, aby wprowadzić tekst.

9C. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

10. Zawiadamianie osób, których dane dotyczą

Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu?

☐ Tak

☐ Nie, ale zostaną zawiadomione
Pamiętaj, że po powiadomieniu osób, należy przesłać treść zawiadomienia do UODO.

☒ Nie, nie zostaną zawiadomione

☐ Nie oceniłem jeszcze

Czy indywidualnie?

☐ Tak

☐ Nie, gdyż indywidualne zawiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został wydany publiczny komunikat lub zastosowano podobny środek, za pomocą którego osoby, których dane dotyczą, zostały poinformowane w równie skuteczny sposób.

Powód niezawiadomienia osób, których dane dotyczą:

Przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony (wskazane w pkt. 9A formularza) i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

Wskaż datę kiedy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu

Kliknij tutaj, aby wprowadzić datę.

Wskaż datę kiedy zamierzasz zawiadomić osoby, których dane dotyczą, o naruszeniu

Kliknij tutaj, aby wprowadzić datę.

☐ Nie znam jeszcze daty kiedy zamierzam zawiadomić osoby, których dane dotyczą

Liczba zawiadomionych osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Po naruszeniu zastosowano środki (wskazane w pkt. 9C formularza) eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Umieść zanonimizowaną treść zawiadomienia, którą przesłałeś bądź zamierzasz przesłać do osób, których dane dotyczą.

Pamiętaj, że zawiadomienie powinno:

- opisywać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosowanych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Kliknij tutaj, aby wprowadzić tekst.

11. Przetwarzanie transgraniczne i inne powiadomienie

☐ Naruszenie ma charakter transgraniczny

Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie:

- | | | | |
|--|-------------------------------------|-------------------------------------|--|
| ☐ Austria | ☐ Belgia | ☐ Bułgaria | ☐ Chorwacja |
| ☐ Cypr | ☐ Czechy | ☐ Dania | ☐ Estonia |
| ☐ Finlandia | ☐ Francja | ☐ Grecja | ☐ Hiszpania |
| ☐ Holandia | ☐ Irlandia | ☐ Islandia | ☐ Liechtenstein |
| ☐ Litwa | ☐ Luksemburg | ☐ Łotwa | ☐ Malta |
| ☐ Niemcy | ☐ Norwegia | ☐ Portugalia | ☐ Rumunia |
| ☐ Słowacja | ☐ Słowenia | ☐ Szwecja | ☐ Węgry |
| ☐ Wielka Brytania | ☐ Włochy | | |

☐ Naruszenie zostało lub zostanie zgłoszone innemu organowi ochrony danych osobowych (opcjonalnie)

Wymień inne organy nadzorcze ochrony danych osobowych, którym naruszenie zostało lub zostanie zgłoszone

☐ Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorcemu z powodu innych zobowiązań prawnych (opcjonalnie)

Np. obowiązek zgłoszenia incydentu wynikający z ustawy o krajowym systemie cyberbezpieczeństwa. Wymień inne organy, którym naruszenie zostało lub zostanie zgłoszone z powodu innych zobowiązań prawnych.

Data, miejscowość

(dla zgłoszenia w formie papierowej)

Podpis osoby lub osób upoważnionych
do reprezentowania administratora⁷
(dla zgłoszenia w formie papierowej)

⁷ Jeżeli zgłoszenie podpisuje pełnomocnik, należy pamiętać o załączeniu pełnomocnictwa

Informacja:

Administrator danych osobowych.

Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:

- a) listownie: ul. Stawki 2, 00-193 Warszawa
- b) przez elektroniczną skrzynkę podawczą dostępną na stronie <https://www.uodo.gov.pl/p/kontakt>
- c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.

Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

Cele i podstawy przetwarzania.

Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust 1, 3 i 4 RODO, podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO¹, a także prowadzenia przez organ wewnętrzny rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.

Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza na platformie E-PUAP bądź Minister Przedsiębiorczości i Technologii w związku z zamieszczeniem formularza na platformie biznes.gov.pl

Okres przechowywania danych.

Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 i art. 58 ust. 2 RODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej – wieczyście.

Prawa osób, których dane dotyczą.

Zgodnie z RODO przysługuje Państwu:

- a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
- b) prawo do sprostowania (poprawiania) swoich danych;
- c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
- d) prawo do ograniczenia przetwarzania danych;
- e) prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.

Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

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 (RODO) oraz podjętych działań.