Zespół Szkół nr 1
ul. Słowackiego 4/10
05 – 400 Otwock

Polityka Bezpieczeństwa Danych Osobowych

Zespół Szkół nr 1 w Otwocku

Opis

Opracowanie omawia sposób przygotowania i zakresu dokumentacji opisującej politykę bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony spełniających wymogi 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).

Polityka Bezpieczeństwa Danych Osobowych w Zespole Szkół nr 1 w Otwocku

Cel i zakres dokumentu

1. Celem Polityki Bezpieczeństwa Danych Osobowych jest zapewnienie bezpieczeństwa danych osobowych, a w szczególności określenie obowiązków i odpowiedzialności osób zobowiązanych do realizacji Instrukcji bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych, przy jednoczesnym spełnieniu wszelkich wymogów obowiązującego prawa.
2. W dokumencie tym zawarto najważniejsze zasady zgodnie z którymi jest realizowany proces ochrony informacji zawierających dane osobowe przetwarzane w Zespole Szkół nr 1 w Otwocku (dalej zwanym „Szkołą").
3. Zasady określone w polityce mają zastosowanie do:

   3.1. Danych osobowych pracowników i byłych pracowników.

   3.2. Danych osobowych współpracowników i byłych współpracowników.

   3.3. Informacji dotyczących bezpieczeństwa danych osobowych, w szczególności nazw kont i haseł we wszystkich systemach, w których mogą się znaleźć informacje zawierające dane osobowe.

   3.4. Innych danych osobowych przetwarzanych w zbiorach danych.

Dokumenty związane

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej zwane: „RODO").
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000).

Definicje

Administrator Danych Osobowych (ADO) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; Administratorem Danych Osobowych jest Dyrektor Szkoły;

Dane biometryczne – dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

Dane dotyczące zdrowia – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (w tym o korzystaniu z usług opieki zdrowotnej), ujawniające informacje o stanie jej zdrowia;

Dane genetyczne – dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

Dane Osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (zgodnie z RODO).

Dostępność informacji – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy istnieje taka potrzeba, tzn. w odpowiednim zakresie, miejscu i czasie (zgodnie z normą PN-ISO/IEC 17799:2003).

Elektroniczny nośnik informacji – materiał lub urządzenie umożliwiające zapisywanie, przechowywanie, przenoszenie i/lub odczytywanie danych w postaci cyfrowej lub analogowej. Przykładami elektronicznych nośników informacji mogą być dyski twarde, pamięci elektroniczne typu flash, dyski CD/DVD/BD, dyskietki i dyski magnetyczne, magnetooptyczne i optyczne, urządzenia przenośne z pamięcią elektroniczną (m.in. telefony komórkowe, urządzenia typu handheld, aparaty cyfrowe, notesy elektroniczne, odtwarzacze multimedialne), itp.

Informacje chronione – informacje sklasyfikowane jako chronione, zgodnie z wymogami obowiązujących aktów prawnych oraz z wewnętrznymi procedurami Szkoły;

Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora Danych Osobowych do nadzorowania oraz przestrzegania zasad ochrony danych osobowych. W przypadku niepowołania IOD, czynności jemu przypisane wykonuje Administrator Danych Osobowych.

Instrukcja Zarządzania – instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych obowiązująca w Szkole;

Integralność informacji – właściwość zapewniająca dokładność i kompletność informacji oraz metod jej przetwarzania.

Naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

Odbiorca danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców;

Ograniczenie przetwarzania – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

Poufność informacji – funkcja bezpieczeństwa zapewniająca, że dostęp do informacji mają tylko osoby upoważnione.

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

Przetwarzanie danych osobowych – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych, w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie, udostępnianie, dopasowywanie, łączenie, ograniczanie, usuwanie lub niszczenie;

Pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (zgodnie z normą PN-I-13335-1).

Strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które mogą przetwarzać dane osobowe z upoważnienia administratora lub podmiotu przetwarzającego;

Tradycyjny nośnik informacji – przedmiot fizyczny niezwiązany z informatyką i komputerami, na którym możliwe jest zapisanie informacji oraz z którego możliwe jest późniejsze odczytanie tej informacji. Przykładami tradycyjnych nośników mogą być wydruki papierowe, folia, taśmy itp.

Usuwanie danych – nieodwracalne zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

Użytkownik – osoba upoważniona do dostępu do zasobów systemu informatycznego posiadająca upoważnienie do przetwarzania danych osobowych w tym systemie. Użytkownikami są podwykonawcy oraz pracownicy etatowi Szkoły;

Zbiór danych osobowych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

Zgoda (osoby, której dane dotyczą) – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

Postanowienia ogólne

1. Za opracowanie niniejszego dokumentu odpowiedzialny jest ADO lub IOD.
2. Za zatwierdzenie niniejszego dokumentu odpowiedzialny jest ADO.
3. Za stosowanie niniejszego dokumentu odpowiedzialni są wszyscy pracownicy i współpracownicy mający dostęp do danych osobowych.
4. Niniejszy dokument stanowi wykonanie obowiązku, o którym mowa w motywie (4) RODO.
5. Polityka Bezpieczeństwa Danych osobowych ustala zbiór opracowań i dokumentów, opisujących szczegółowo sposób zabezpieczenia danych osobowych oraz zabezpieczeń użytych w systemach informatycznych, zapewniających ochronę przetwarzanych danych osobowych, w tym:
   a. wskazanie obszaru, w którym przetwarzane są dane osobowe;
   b. wykaz zbiorów danych osobowych i programów zastosowanych do przetwarzania danych osobowych;
   c. opis struktury zbioru, zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi;
   d. sposób przepływu danych osobowych pomiędzy systemami;
   e. środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności, i rozliczalności przetwarzanych danych osobowych;
   f. procedurę postępowania w przypadku wystąpienia naruszenia – tzw. system reakcji na incydenty;
   g. ścieżkę postępowania w przypadku wystąpienia wniosku informacyjnego od osoby, której dane dotyczą;
   h. ścieżkę postępowania w przypadku złożenia sprzeciwu co do przetwarzania danych osobowych do celów marketingu bezpośredniego;
   i. wymogi zapewniające spełnienie obowiązków informacyjnych oraz praw osób, których dane dotyczą, w tym „prawa do bycia zapomnianym”;
   j. zasady privacy by design oraz privacy by default;
   k. notyfikację organowi nadzorczemu wystąpienia incydentu w zakresie przetwarzania danych osobowych;
   l. notyfikację osobie, której dane dotyczą incydentu dotyczącego naruszenia lub wycieku danych jej dotyczących;
   m. prawo do przenoszalności danych;
   n. ocenę skutków dla przetwarzania danych osobowych (privacy impact assessment).

Realizacja podstawowych wymogów Polityki

Obowiązek informacyjny

1. Szkoła zbiera dane osobowe zarówno od osoby, której dane dotyczą, jak i od innych osób.
2. Szkoła zobowiązana jest poinformować tę osobę o:
    a) pełnej nazwie i adresie swojej siedziby,
    b) celu zbierania danych, w szczególności o znanych jej, w czasie udzielania informacji, odbiorcach lub przewidywanych odbiorcach, lub kategoriach odbiorców danych,
    c) prawie dostępu do treści swoich danych oraz ich poprawiania,
    d) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje – o jego podstawie prawnej.

Wzór informacji dla osoby, której dane dotyczą zawiera załącznik nr 7 do Polityki Bezpieczeństwa.

3. Obowiązek informacyjny wypełniany jest w chwili zbierania danych. Nie ma znaczenia sposób zbierania danych.
4. W przypadku zbierania danych nie od osoby, której one dotyczą, ADO zobowiązany jest poinformować tę osobę dodatkowo o źródle, z którego pozyskane są dane oraz prawie do wniesienia żądania zaprzestania przetwarzania danych, sprzeciwu wobec ich przetwarzania lub przekazywania ich innemu administratorowi.
5. Informacje stanowiące dane osobowe mogą być przekazywane, przez umocowanych do tego typu czynności pracowników, wyłącznie osobom, których te dane dotyczą, chyba że osoby te wyrażą zgodę na przekazywanie danych ich dotyczących wskazanym przez siebie osobom lub podmiotom.
6. Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
7. Wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa do usunięcia danych.
8. Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
9. Jeżeli określony zestaw danych osobowych odnosi się do więcej niż jednej osoby, której dane dotyczą, prawo do otrzymania danych osobowych nie powinno powodować uszczerbku dla praw i wolności innych osób, których dane dotyczą.

10. Osoba, której dane dotyczą, ma prawo żądać, aby jej dane zostały niezwłocznie usunięte, jeżeli:
    a. nie są one już niezbędne do celów, w których były przetwarzane;
    b. wycofała zgodę i nie ma innych podstaw, aby przetwarzać jej dane;
    c. wnosi sprzeciw;
    d. Szkoła przetwarzała dane bez podstawy prawnej;
    e. Szkoła ma usunąć dane, aby wywiązać się z obowiązku prawnego lub zbierała dane w związku z usługami tzw. społeczeństwa informacyjnego, kierowanymi bezpośrednio do dzieci (np. portale internetowe).

Jeżeli któryś z tych warunków jest spełniony, administrator danych musi usunąć dane bez zbędnej zwłoki („prawo do bycia zapomnianym").

11. W sytuacji opisanej w pkt 10, dane usuwane są w sposób nie pozwalający na ich odczytanie i odzyskanie z powrotem. Dane usuwane są z bazy trwale lub nadpisywane innymi wartościami (np. ciągiem znaków, tzw. anonimizacja).
12. W sytuacji opisanej w pkt 10, jeżeli (nazwa) upubliczniła dane, ma obowiązek poinformowania innych administratorów, że dana osoba żąda, aby usunęli wszelkie łącza do tych danych, ich kopie lub replikacje.
13. Dane usuwane są niezwłocznie, chyba że ich przetwarzanie jest niezbędne do:
    a. korzystania z prawa do wolności wypowiedzi i informacji,
    b. wywiązania się z prawnego obowiązku, któremu podlega administrator,
    c. wykonania zadania w interesie publicznym lub w ramach władzy publicznej (w dziedzinie zdrowia publicznego, w celach archiwalnych, statystycznych, badań naukowych lub historycznych, jak też do ustalenia, dochodzenia lub obrony roszczeń) – do czasu rozwiązania sporu.

Obszar przetwarzania danych osobowych w Zespole Szkół nr 1 w Otwocku

1. Szczegółowy „Wykaz budynków, pomieszczeń lub części pomieszczeń w których przetwarzane są dane osobowe" stanowi **Załącznik nr 1** do niniejszego dokumentu i zawiera następujące informacje:
    a. określenie obiektu;
    b. lokalizacja (adres i nr budynku).
2. Obiekty, w których przetwarzane są dane osobowe, są zabezpieczone w sposób zapewniający rozliczalność i poufność przetwarzanych danych.

Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe

1. Obszarem przetwarzania danych osobowych są pomieszczenia, w których są przetwarzane dane osobowe zarówno w formie papierowej, jak i w systemie informatycznym.
2. Wszelkie zmiany dotyczące obszaru przetwarzania danych osobowych muszą być na bieżąco przekazywane do Inspektora Ochrony Danych.
3. Obszar przetwarzania danych osobowych posiada następujące zabezpieczenia:

Miejsce przetwarzania danych osobowych	Zastosowane zabezpieczenia fizyczne
Adres **ul. Słowackiego 4/10** **05 – 400 Otwock**	**Kamery CCTV**
	Ochrona 24/7 (dozorca)
	Kraty w części pomieszczeń administracyjnych
	Szafki niemetalowe
	Szafki metalowe
	Sejf
	Niszczarka
	Gaśnica
	Szyfrowane laptopy
	Karty/czytnik dostępu do pomieszczeń

4. Przebywanie wewnątrz obszaru przetwarzania danych osobowych osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub na podstawie wydanego upoważnienia do przebywania w obszarze.
5. Osoby upoważnione do przetwarzania danych osobowych oraz osoby upoważnione do przebywania w obszarze przetwarzania danych osobowych zobowiązane są do przestrzegania następujących zasad:
    a. ruch osób z zewnątrz w wymienionym obszarze odbywa się pod kontrolą osób upoważnionych;
    b. zabronione jest pozostawianie osób trzecich w obszarze bez nadzoru osoby upoważnionej;

c. na czas nieobecności osób upoważnionych pomieszczenia i budynki powinny być zamykane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym;

d. monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić osobom postronnym wgląd w te dane;

e. dokumenty z danymi osobowymi powinny być zamykana na klucz w nieprzeszklonych meblach biurowych (szuflady, szafy).

Wykaz zbiorów danych osobowych i programów zastosowanych do przetwarzania danych osobowych

1. Zbiory danych osobowych przetwarzane w Szkole dzieli się na:
   a. wewnętrzne – zbiory dotyczące danych osób zatrudnionych w Szkole;
   b. zewnętrzne – zbiory dotyczące danych osób, które nie są zatrudnione w Szkole, ale ich dane osobowe przetwarzane są w związku z realizacją statutowych zadań, zgodnie z wymogami obowiązującego prawa;
   c. doraźne – zbiory tworzone do jednorazowego wykorzystania, a następnie niszczone.
2. Wykaz zbiorów danych osobowych stanowi **Załącznik nr 2** „Wykaz zbiorów danych osobowych przetwarzanych w Szkole" i zawiera następujące informacje:
   a. nazwa zbioru/zasobu danych osobowych;
   b. cel przetwarzania zbioru/zasobu;
   c. opis struktury, pola informacyjne, zakres danych osobowych w zbiorze/zasobie;
   d. systemy przetwarzania (nazwa systemu, programu, sposób przechowywania informacji);
   e. podstawa prawna przetwarzania;
   f. podmioty, którym powierzane są dane osobowe;
   g. podmioty, którym udostępniane są dane osobowe;
   h. retencja danych osobowych w organizacji;
   i. sposób zbierania danych osobowych;
   j. czy zbierane są zgody na przetwarzanie danych osobowych.

Opis struktury zbiorów, zawartości poszczególnych pól informacyjnych i powiązania pomiędzy nimi

1. Zgodnie z art. 13 i art. 24 RODO, dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze.

2. Opis struktury zbiorów znajduje się w Załączniku nr 2 „Wykaz zbiorów danych osobowych przetwarzanych w Zespole Szkół nr 1 w Otwocku" oraz w Instrukcji zarządzania systemem informatycznym.

3. Struktura zbiorów ma postać płaską lub wielowymiarową.

Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami

1. Przepływ danych osobowych pomiędzy systemami odbywać się może jedynie za zgodą IOD. Zgoda może być wyrażona w postaci pisemnej lub ustnej.
2. Przepływ danych osobowych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
3. Dane osobowe mogą być przenoszone pomiędzy systemami w sposób manualny bądź zautomatyzowany.

Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

1. Zgodnie z art. 25 ust. 1 RODO, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości, zakresu przetwarzania, okresu przechowywania oraz dostępności zbieranych danych osobowych. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

2. Szczegółowe omówienie środków zabezpieczenia organizacyjnego i technicznego znajduje się w Polityce Bezpieczeństwa Danych Osobowych oraz w Instrukcji zarządzania systemem informatycznym.

Zarządzanie przetwarzaniem danych osobowych oraz rola Inspektora Ochrony Danych

1. IOD nadzoruje przestrzeganie obowiązków zabezpieczenia danych osobowych oraz zasad ochrony danych osobowych, określonych przez administratora danych, stosując odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i

organizacyjne, które mają zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. W pojęciu tych obowiązków mieści się również obowiązek wdrożenia dokumentacji (tj. niniejszej Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania systemem informatycznym) określonej w przepisach wykonawczych do ustawy oraz występowanie z inicjatywami zmian tych dokumentów, stosownie do zmieniających się zagrożeń przetwarzania danych osobowych. Do zadań IOD należy w szczególności:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO;
b) monitorowania przestrzegania RODO, innych przepisów Unii, ustawy o ochronie danych osobowych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
d) współpraca z administratorem danych osobowych.

2. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Przetwarzanie danych osobowych w systemach informatycznych

1. Dane osobowe mogą być przetwarzane wyłącznie w systemach spełniających wymogi RODO.
2. System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie:
    a. daty pierwszego wprowadzenia danych do systemu;
    b. identyfikatora użytkownika wprowadzającego dane osobowe do systemu;
    c. źródła danych – w przypadku zbierania danych nie od osoby, której one dotyczą;
    d. informacji o odbiorcach w rozumieniu art. 4 pkt 9 RODO, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.
3. Jeżeli przetwarzanie danych odbywa się na podstawie zgody osoby, której dane dotyczą lub umowy, której stroną jest osoba, której dane dotyczą oraz przetwarzanie odbywa się w sposób zautomatyzowany, osoba ta ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi oraz przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora.

4. System informatyczny służący do przetwarzania danych osobowych jest wyposażony w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych (na poziomie samej aplikacji lub na poziomie logowania do systemu/domeny).
5. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego przydzielany innej osobie.
6. Konto w systemie informatycznym osoby, która utraciła uprawnienia dostępu do danych osobowych, powinno być niezwłocznie zablokowane, w celu zapobieżenia dalszemu dostępowi tej osoby do danych osobowych.
7. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przed utratą poprzez wykonywanie kopii zapasowych.
8. Szczegółowe zasady przyznawania identyfikatorów i haseł dostępowych, sporządzania kopii zapasowych oraz odnotowywania informacji określone są w Instrukcji zarządzania systemem informatycznym.
9. Ochrona prywatności danych osobowych zapewniana jest na każdym etapie ich przetwarzania, w tym w fazie projektowania, poprzez jej wbudowanie w architekturę systemu, jak i procesy, które system obsługuje (jak najszybsza pseudonimizacja danych, umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych).

Zasady zarządzania systemami informatycznymi

1. Zasady zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych określa szczegółowo Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, w zakresie:
    a. procedur nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazania osoby odpowiedzialnej za te czynności;
    b. stosowanych metod i środków uwierzytelnienia oraz procedur związanych z ich zarządzaniem i użytkowaniem;
    c. procedur rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonych dla użytkowników systemu;
    d. procedur tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
    e. sposobu, miejsca i okresu przechowywania:
        i. elektronicznych nośników informacji zawierających dane osobowe,
        ii. kopii zapasowych zbiorów danych.

f. sposobu zabezpieczenia systemu informatycznego przed:

i. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,

ii. działaniem oprogramowania powodującego utratę danych,

iii. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;

g. sposobu realizacji wymogów dotyczących odnotowywania i wydruku informacji zawierających dane osobowe;

h. procedur wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

2. Za stworzenie i aktualizację instrukcji wymienionej w pkt 1 odpowiada IOD.

Przetwarzanie danych osobowych znajdujących się na nośnikach papierowych

1. Dane osobowe zawarte w dokumentacji papierowej przetwarzane są przez osoby upoważnione zgodnie z zasadami niniejszej Polityki Bezpieczeństwa Danych Osobowych.
2. Do przetwarzania dokumentów papierowych z danymi osobowymi konieczne jest zastosowanie środków ochrony dotyczących obszaru przetwarzania danych osobowych.
3. Niszczenia dokumentów papierowych z danymi osobowymi przetwarzanymi w Szkole dla celów doraźnych, dokonują pracownicy upoważnieni do przetwarzania danych osobowych, w sposób uniemożliwiający ich odczytanie (przy użyciu niszczarek znajdujących się na terenie Szkoły).

Przetwarzanie danych osobowych znajdujących się na nośnikach elektronicznych

1. Dane osobowe zawarte na nośnikach elektronicznych przetwarzane są zgodnie z zasadami zawartymi w Polityce Bezpieczeństwa Danych Osobowych wyłącznie przez osoby upoważnione.
2. Osoby upoważnione, które otrzymały sprzęt elektroniczny do realizacji obowiązków, odpowiedzialne są za powierzone mienie.
3. Zapisywanie danych osobowych na nośnikach elektronicznych jest możliwe wyłącznie za zgodą wykonujących obowiązki ADO lub IOD w następujących przypadkach:

a. tworzenie informacji celem wykonania przepisów ustawowych;

b. tworzenie kopii doraźnych na potrzeby wewnętrzne danej komórki;

c. tworzenie kopii zapasowych;

4. Za wykonywanie i przechowywanie kopii zapasowych odpowiedzialni są użytkownicy stanowisk komputerowych, na których dyskach lokalnych znajdują się dane osobowe.
5. IOD lub wyznaczony pracownik odpowiedzialny za obsługę informatyczną (ASI) określa częstotliwość tworzenia, miejsce przechowywania i sposób ewidencjonowania kopii zapasowych plików z danymi osobowymi, znajdujących się na dyskach lokalnych pracowników oraz typ nośnika, na którym wykonuje się kopię.
6. Tworzenie kopii danych osobowych doraźnych na dowolnym nośniku może się odbywać za zgodą Administratora Danych Osobowych lub Inspektora Ochrony Danych.
7. Do przetwarzania danych osobowych na nośnikach elektronicznych konieczne jest zastosowanie środków ochrony dotyczących obszaru przetwarzania danych osobowych.
8. Każda osoba mająca dostęp do nośników elektronicznych z danymi osobowymi, bez względu na sposób ich wykorzystywania, jest odpowiedzialna za ich ochronę.
9. W sytuacji, gdy przechowywanie kopii doraźnych danych osobowych lub kopii stworzonych w celach wymiany informacji jest już zbędne ze względu na cel ich utworzenia, pracownik posiadający kopie jest zobowiązany do:
   a. wykasowania danych z nośnika wielokrotnego użytku;
   b. zniszczenia nośnika jednokrotnego użytku w sposób uniemożliwiający odczytanie danych.
10. Zużyte lub uszkodzone nośniki, na których zapisane były dane osobowe, niszczy się w sposób uniemożliwiający ich odczytanie.
11. Zużyte lub uszkodzone nośniki, na których tworzono kopie zapasowe zbiorów danych, niszczone są przez wyznaczonego przez ADO, pracownika w sposób uniemożliwiający ich odczytanie.

Ocena skutków dla przetwarzania danych osobowych

1. Zgodnie z art. 35 RODO, podstawowym celem analizy skutków dla przetwarzania danych osobowych jest zapewnienie zgodności procesów przetwarzania z RODO, identyfikacja ewentualnych zagrożeń oraz ograniczenie naruszeń prywatności.
2. ADO ma obowiązek dokonania oceny w sytuacji, gdy planowane przetwarzanie ze względu na swój charakter, zakres, kontekst czy cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, których dane dotyczą. Ryzyko naruszenia odnosi się przede wszystkim do prawa do prywatności, wolności wypowiedzi, wolności i swobody przekonań, swobody poruszania się, zakazu dyskryminacji, swobody myśli oraz poglądów religijnych.

3. Zastosowanie mechanizmu oceny jest konieczne w przypadku spełnienia przynajmniej dwóch z następujących przesłanek:
    a) przetwarzanie oparte jest o automatyczną ocenę czynników osobowych odnoszących się do osób fizycznych, w tym profilowanie i jest podstawą decyzji wywołujących skutki prawne wobec tych osób lub w podobny sposób znacząco wpływających na te osoby;
    b) przetwarzane są dane osobowe szczególnej kategorii (dane wrażliwe);
    c) przetwarzanie uwzględnia systematyczny monitoring na dużą skalę miejsc dostępnych publicznie;
    d) przetwarzanie zakłada łączenie różnych zbiorów danych, np. pozyskanych do różnych celów;
    e) przetwarzane mają być dane osób, które mogą mieć trudności z wyrażeniem sprzeciwu, np. dzieci czy pracowników podporządkowanych pracodawcy;
    f) przetwarzanie zakłada wykorzystanie innowacyjnych technologii czy środków organizacyjnych;
    g) operacje przetwarzania mogą utrudniać osobom, których dane dotyczą, wykonywanie przysługujących im praw.
4. W sytuacji spełnienia tylko jednej przesłanki, zastosowanie oceny skutków przetwarzania będzie możliwe, pod warunkiem, że będzie to uzasadnione okolicznościami danego przypadku.
5. Ocena skutków przetwarzania nie jest wymagana, gdy przetwarzanie nie prowadzi do wysokiego naruszenia praw i wolności osób, których dane dotyczą, a:
    a) zostało już dopuszczone w bardzo podobnym procesie przetwarzania;
    b) ma podstawę prawną w prawie UE lub prawie państwa członkowskiego.
6. Ocena skutków przetwarzania danych osobowych może być przeprowadzana dla pojedynczych operacji przetwarzania danych. Możliwe jest również przeprowadzanie jednej oceny dla kilku podobnych operacji, wiążących się ze zbliżonym ryzykiem dla praw i wolności podmiotów danych. Ocena ta jednak musi być przeprowadzona przed planowanym rozpoczęciem przetwarzania danych.
7. ADO ma obowiązek przeprowadzenia z IOD konsultacji. Powinien również zasięgnąć opinii osób, których dane dotyczą lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych, publicznych lub bezpieczeństwa operacji przetwarzania.
8. W razie ryzyka wynikającego z operacji przetwarzania, ocena jego skutków przeprowadzana jest okresowo i uaktualniana.

Odpowiedzialność karna

Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi określonymi w art. 83 RODO oraz art. 266 – 269, 287 kodeksu karnego.

Postanowienia końcowe

1. Niniejsza Polityka Bezpieczeństwa Danych Osobowych jest dokumentem wewnętrznym i własnością Szkoły, a tym samym nie może być udostępniana osobom innym niż pracownicy i współpracownicy w żadnej formie, bez zgody Inspektora Ochrony Danych.
2. Każdy pracownik, współpracownik przed uzyskaniem dostępu do danych osobowych w Szkole zobowiązany jest zapoznać się z postanowieniami niniejszej Polityki Bezpieczeństwa Danych Osobowych.
3. Polityka Bezpieczeństwa Danych Osobowych powinna być poddawana regularnemu przeglądowi, a w przypadku istotnych zmian powinna zapewniać, że pozostaje przydatna, adekwatna i skuteczna.
4. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO.

Dokumenty powiązane

1. Załącznik nr 1: Wykaz budynków, w których przetwarzane są dane osobowe.
2. Załącznik nr 2: Wykaz zbiorów danych osobowych przetwarzanych w Zespole Szkół nr 1 w Otwocku.
3. Załącznik nr 3: Instrukcja nadawania upoważnień do przetwarzania danych osobowych.
4. Załącznik nr 4: Instrukcja postępowania w przypadku wystąpienia naruszenia.
5. Załącznik nr 5: Procedura postępowania w przypadku wystąpienia wniosku informacyjnego od osoby, której dane dotyczą.
6. Załącznik nr 6: Procedura postępowania w przypadku złożenia sprzeciwu co do przetwarzania danych osobowych do celów marketingu bezpośredniego.
7. Załącznik nr 7: Klauzula obowiązku informacyjnego.
8. Instrukcja Bezpieczeństwa Systemu Informatycznego.

Wykaz budynków, w których przetwarzane są dane osobowe

1. W Szkole zostały określone budynki i pomieszczenia, w których przetwarzane są dane osobowe.
2. Obszarem przetwarzania danych osobowych dla zbiorów będących w kompetencji Szkoły są budynki administrowane lub wynajmowane przez Szkołę.
3. Warunki dotyczące bezpieczeństwa przetwarzania danych osobowych w budynkach zostały określone w „Polityce Bezpieczeństwa Danych Osobowych".
4. Wykaz budynków i lokali administrowanych przez Szkołę:

Opis	Kraj	Miasto	Adres	Lokale
Siedziba główna	**Polska**	**05-400 Otwock**	**ul. Słowackiego 4/10**	**Wszystkie pomieszczenia administracyjne**

Wykaz zbiorów danych osobowych przetwarzanych w Zespole Szkół nr 1 w Otwocku

1. Dla każdego zidentyfikowanego w Szkole zbioru danych osobowych, wskazano opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze.
2. W Szkole prowadzony jest Rejestr Czynności Przetwarzania Danych.
3. Wykaz zbiorów danych osobowych przetwarzanych w Szkole został wylistowany w poniższych tabelach.
4. Opis struktury zbiorów i zakres informacji gromadzonych w poszczególnych zbiorach przetwarzanych w Szkole.

Zbiór nr 1

Wymaganie	Opis
Nazwa zbioru	**Kadry**
Cel przetwarzania zbioru	Rekrutacja i świadczenie pracy na rzecz Szkoły.
Pola informacyjne przetwarzane w zbiorze	Imię/imiona, nazwisko, nazwisko rodowe, data urodzenia, adres zamieszkania, inf. o wynagrodzeniu, inf. o wykształceniu, PESEL, NIP, nr telefonu, stan rodzinny, inf. o stosunku do obowiązku obrony, dane osoby, którą należy zawiadomić w razie wypadku, seria i nr dokumentu tożsamości, data oraz przez kogo wydany dokument tożsamości, inf. o zaległościach komorniczych
Sposób gromadzenia danych oraz systemy użyte do ich przetwarzania	Wersja papierowa: teczki akt osobowych, kwestionariusze osobowe, wykaz pracowników do zaświadczenia lekarskiego, CV Wersja elektroniczna: MS Office, LibreOffice, e-Dziennik Librus, SIO, Arkusz Optivum

Data wpisu zbioru do rejestru	25.05.2018 r.
oznaczenie podmiotu, któremu udostępnia się przetwarzanie danych ze zbioru i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	1. Oświata Powiatowa w Otwocku ul. Poniatowskiego 10, 05 – 400 Otwock; 2. Kuratorium Oświaty; 3. lekarze medycyny pracy; 4. ZUS
oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	1. Ośrodek Szkoleń i Doradztwa BHP i P. POŻ. „KASK”, ul. Rysia 16, 05 – 400 Otwock 2. Vulcan Sp. z o. o. ul. Wołowska 6, 51 – 116 Wrocław 3. Librus Sp. z o. o. Sp. k. ul. Korfantego 193, 40 – 153 Katowice
podstawa prawna upoważniająca do prowadzenia zbioru danych;	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. 2017 poz. 59); Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. 2017 poz. 2198); Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. 2018 poz. 108).
Typ danych;	Dane pracowników
Retencja danych osobowych w organizacji	50 lat na podstawie przepisów prawa
sposób zbierania danych do zbioru, w szczególności informacja czy dane do zbioru są zbierane od osób, których dotyczą;	Od osób, których dane dotyczą; Od innych osób
sposób udostępniania danych ze zbioru, w szczególności informacja czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa;	Nie
oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;	Pracownicy Szkoły, Oświata Powiatowa w Otwocku, Kuratorium Oświaty, lekarze medycyny pracy, ZUS, Ośrodek Szkoleń i Doradztwa BHP i P. POŻ. „KASK”
informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego.	Nie

Czy zbierane są zgody na przetwarzanie danych osobowych	TAK
Inspektor Ochrony Danych	PerfectInfo Paweł Maliszewski ul. Skowronia 32, 05-270 Marki Tel. 606 191 915

Zbiór nr 2

Wymaganie	**Opis**
Nazwa zbioru	**Zakładowy Fundusz Świadczeń Socjalnych**
Cel przetwarzania zbioru	Świadczenie wsparcia finansowego dla pracowników Szkoły.
Pola informacyjne przetwarzane w zbiorze	Imię, nazwisko, adres zamieszkania, nr rachunku bankowego, wysokość dochodu na członka rodziny, nr telefonu
Sposób gromadzenia danych oraz systemy użyte do ich przetwarzania	Wersja papierowa: wnioski Wersja elektroniczna: brak

Data wpisu zbioru do rejestru	25.05.2018 r.
oznaczenie podmiotu, któremu udostępnia się przetwarzanie danych ze zbioru i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	Oświata Powiatowa w Otwocku ul. Poniatowskiego 10, 05 – 400 Otwock
oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	brak
podstawa prawna upoważniająca do prowadzenia zbioru danych;	Ustawa z dnia 4 marca 1994 r. o Zakładowym Funduszu Świadczeń Socjalnych.
Typ danych;	Dane pracowników i byłych pracowników
Retencja danych osobowych w organizacji	5 lat na podstawie przepisów prawa
sposób zbierania danych do zbioru, w szczególności informacja czy dane do zbioru są zbierane od osób, których dotyczą;	Od osób, których dane dotyczą Od innych osób
sposób udostępniania danych ze zbioru, w szczególności informacja czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa;	Nie
oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;	Pracownicy Szkoły, Oświata Powiatowa w Otwocku
informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego.	Nie
Czy zbierane są zgody na przetwarzanie danych osobowych	Nie dotyczy
Inspektor Ochrony Danych	PerfectInfo Paweł Maliszewski ul. Skowronia 32, 05-270 Marki Tel. 606 191 915

Zbiór nr 3

Wymaganie	Opis
Nazwa zbioru	**Księgowość**
Cel przetwarzania zbioru	Zarządzanie fakturami oraz danymi kontaktowymi z faktur (w tym danymi pracowników firm zewnętrznych podpisujących faktury).
Pola informacyjne przetwarzane w zbiorze	Imię, nazwisko, nr telefonu, dane teleadresowe firmy, adres e-mail, NIP, nr rachunku bankowego
Sposób gromadzenia danych oraz systemy użyte do ich przetwarzania	Wersja papierowa: faktury, listy płac Wersja elektroniczna: MS Office, LibreOffice, Księgowość Optivum

Data wpisu zbioru do rejestru	25.05.2018 r.
oznaczenie podmiotu, któremu udostępnia się przetwarzanie danych ze zbioru i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	Oświata Powiatowa w Otwocku ul. Poniatowskiego 10, 05 – 400 Otwock
oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	Vulcan Sp. z o. o. ul. Wołowska 6, 51 – 116 Wrocław
podstawa prawna upoważniająca do prowadzenia zbioru danych;	Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz. U. 2018 poz. 395)
Typ danych;	Dane pracowników i kontrahentów
Retencja danych osobowych w organizacji	Dane pracowników – 50 lat na podstawie przepisów prawa; dane kontrahentów – na podstawie zawartej umowy
sposób zbierania danych do zbioru, w szczególności informacja czy dane do zbioru są zbierane od osób, których dotyczą;	Od osób, których dane dotyczą Od innych osób
sposób udostępniania danych ze zbioru, w szczególności informacja czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa;	Nie
oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;	Pracownicy Szkoły, Oświata Powiatowa w Otwocku
informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego.	Nie
Czy zbierane są zgody na przetwarzanie danych osobowych	Nie dotyczy
Inspektor Ochrony Danych	PerfectInfo Paweł Maliszewski ul. Skowronia 32, 05-270 Marki Tel. 606 191 915

Zbiór nr 4

Wymaganie	Opis
Nazwa zbioru	**Uczniowie**
Cel przetwarzania zbioru	Realizacja obowiązku oświatowego.
Pola informacyjne przetwarzane w zbiorze	Imię/imiona, nazwisko, data i miejsce urodzenia, PESEL, adres zamieszkania, inf. o niepełnosprawności, inf. o stanie zdrowia, dane rodziców/opiekunów prawnych (imiona i nazwisko, adres zamieszkania/zameldowania, miejsce pracy, nr telefonu, adres e-mail), inf. o potrzebie indywidualnego nauczania
Sposób gromadzenia danych oraz systemy użyte do ich przetwarzania	Wersja papierowa: księga uczniów, karty zdrowia, zaświadczenia lekarskie, opinie z poradni psychologiczno – pedagogicznej, opinie o potrzebie indywidualnego nauczania Wersja elektroniczna: SIO, MS Office, LibreOffice, Mol Optivum, e-Dziennik Librus

Data wpisu zbioru do rejestru	25.05.2018 r.
oznaczenie podmiotu, któremu udostępnia się przetwarzanie danych ze zbioru i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	Oświata Powiatowa w Otwocku ul. Poniatowskiego 10, 05 – 400 Otwock
oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	1. Librus Sp. z o. o. Sp. K. ul. Korfantego 193, 40 – 153 Katowice 2. Vulcan Sp. z o. o., ul. Wołowska 6 51 – 116 Wrocław
podstawa prawna upoważniająca do prowadzenia zbioru danych;	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. 2017 poz. 59); Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. 2017 poz. 2198).
Typ danych;	Dane uczniów i ich rodziców
Retencja danych osobowych w organizacji	Dzienniki – 25 lat; arkusze ocen – 50 lat na podstawie Jednolitego Rzeczowego Wykazu Akt
sposób zbierania danych do zbioru, w szczególności informacja czy dane do zbioru są zbierane od osób, których dotyczą;	Od osób, których dane dotyczą, Od innych osób
sposób udostępniania danych ze zbioru, w szczególności informacja czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa;	Nie
oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;	Pracownicy Szkoły, Oświata Powiatowa w Otwocku, Librus Sp. z o. o. Sp. K.
informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego.	Nie
Czy zbierane są zgody na przetwarzanie danych osobowych	Tak

Inspektor Ochrony Danych	PerfectInfo Paweł Maliszewski ul. Skowronia 32, 05-270 Marki Tel. 606 191 915

Zbiór nr 5

Wymaganie	**Opis**
Nazwa zbioru	**Rodzice/opiekunowie prawni**
Cel przetwarzania zbioru	Informowanie rodziców/opiekunów prawnych o sprawach związanych z dziećmi.
Pola informacyjne przetwarzane w zbiorze	Imię, nazwisko, adres zamieszkania, nr telefonu, adres e-mail, miejsce pracy
Sposób gromadzenia danych oraz systemy użyte do ich przetwarzania	Wersja papierowa: wnioski o przyjęcie do szkoły Wersja elektroniczna: brak

Data wpisu zbioru do rejestru	25.05.2018 r.
oznaczenie podmiotu, któremu udostępnia się przetwarzanie danych ze zbioru i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	brak
oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	brak
podstawa prawna upoważniająca do prowadzenia zbioru danych;	Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. 2017 poz. 2198)
Typ danych;	Dane rodziców/opiekunów prawnych
Retencja danych osobowych w organizacji	Na czas uczęszczania dziecka do szkoły
sposób zbierania danych do zbioru, w szczególności informacja czy dane do zbioru są zbierane od osób, których dotyczą;	Od osób, których dane dotyczą Od innych osób
sposób udostępniania danych ze zbioru, w szczególności informacja czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa;	Nie
oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;	Pracownicy Szkoły
informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego.	Nie
Czy zbierane są zgody na przetwarzanie danych osobowych	Tak
Inspektor Ochrony Danych	PerfectInfo Paweł Maliszewski ul. Skowronia 32, 05-270 Marki Tel. 606 191 915

Zbiór nr 6

Wymaganie	Opis
Nazwa zbioru	**Uczestnicy konkursów ze Szkoły oraz innych placówek oświatowych**
Cel przetwarzania zbioru	Organizowanie konkursów na poziomie powiatowym
Pola informacyjne przetwarzane w zbiorze	Imię, nazwisko, szkoła, do której uczęszcza uczestnik
Sposób gromadzenia danych oraz systemy użyte do ich przetwarzania	Wersja papierowa: zgody, zgłoszenia na konkursy, protokoły Wersja elektroniczna: MS Office

Data wpisu zbioru do rejestru	25.05.2018 r.
oznaczenie podmiotu, któremu udostępnia się przetwarzanie danych ze zbioru i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	brak
oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	brak
podstawa prawna upoważniająca do prowadzenia zbioru danych;	1. Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. 2017 poz. 2198); 2. Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 29 stycznia 2002 r. w sprawie organizacji oraz sposobu przeprowadzania konkursów, turniejów i olimpiad (Dz. U. 2002 poz. 125); 3. Rozporządzenie Ministra Edukacji Narodowej z dnia 18 sierpnia 2017 r. zmieniające rozporządzenie w sprawie organizacji oraz sposobu przeprowadzania konkursów, turniejów i olimpiad (Dz. U. 2017 poz. 1580); 4. Rozporządzenie Ministra Edukacji Narodowej z dnia 3 sierpnia 2017 r. w sprawie oceniania, klasyfikowania i promowania uczniów i słuchaczy w szkołach publicznych (Dz. U. 2017 poz. 1534);
Typ danych;	Dane uczniów biorących udział w konkursach
Retencja danych osobowych w organizacji	1 rok
sposób zbierania danych do zbioru, w szczególności	Od osób, których dane dotyczą

informacja czy dane do zbioru są zbierane od osób, których dotyczą;	Od innych osób
sposób udostępniania danych ze zbioru, w szczególności informacja czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa;	Nie
oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;	Pracownicy Szkoły
informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego.	Nie
Czy zbierane są zgody na przetwarzanie danych osobowych	Tak
Inspektor Ochrony Danych	PerfectInfo Paweł Maliszewski ul. Skowronia 32, 05-270 Marki Tel. 606 191 915

Instrukcja nadawania upoważnień do przetwarzania danych osobowych w Zespole Szkół nr 1 w Otwocku

1. Niniejsza „Instrukcja nadawania upoważnień do przetwarzania danych osobowych w Zespole Szkół nr 1 w Otwocku", zwana dalej „Instrukcją", stanowi uzupełnienie Polityki Bezpieczeństwa Danych Osobowych przetwarzanych w Szkole i stanowi wykonanie art. 24 i art. 29 RODO.
2. Instrukcja dotyczy również nadawania upoważnień do przetwarzania danych osobowych użytkownikom zewnętrznym oraz innym osobom, które z racji wykonywanej pracy na rzecz Szkoły mają dostęp do danych osobowych przetwarzanych w Szkole.
3. Celem instrukcji jest ustalenie jednolitych zasad postępowania w przypadku:
    a) dopuszczenia osób do przetwarzania danych osobowych;
    b) obowiązków osób dopuszczonych do przetwarzania danych osobowych;
    c) zasad blokowania dostępu pracownika do zbiorów danych z danymi osobowymi w przypadku stwierdzenia braku jego wiarygodności.
4. Do stosowania niniejszej instrukcji zobowiązani są wszyscy pracownicy Szkoły, zarówno upoważnieni do przetwarzania danych osobowych i pracujący w obszarze przetwarzania danych osobowych, jak również osoby upoważnione do przetwarzania danych osobowych na podstawie stosownych umów.
5. Wykonujący obowiązki ADO odpowiada za przestrzeganie przepisów RODO, w szczególności:
    a) upoważnia osoby do przetwarzania danych osobowych w administrowanych zbiorach zgodnie z art. 24 RODO;
    b) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w administrowanych zbiorach; wzór ewidencji upoważnień stanowi załącznik nr 3.
6. Do przetwarzania danych osobowych zgromadzonych w zbiorach i ewidencjach w Szkole mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez wykonującego obowiązki Administratora Danych.
7. Z wnioskiem o wydanie upoważnienia, o którym mowa w pkt. 6, występuje bezpośredni przełożony osoby, która realizować będzie zadania związane z przetwarzaniem danych osobowych w Szkole.

8. Przed uzyskaniem upoważnienia, o którym mowa w pkt. 6, wykonujący obowiązki Administratora Danych nie może dopuścić użytkownika do przetwarzania danych osobowych w Szkole.
9. Administrator Danych oraz wykonujący obowiązki Administratora mogą odmówić wydania upoważnienia do przetwarzania danych osobowych w przypadku, gdy osoba, w stosunku do której złożono wniosek o wydanie upoważnienia, nie gwarantuje ochrony danych osobowych w szczególności w zakresie nieuprawnionego ich udostępnienia osobom nieupoważnionym, przetwarzania z naruszeniem ustawy oraz utratą, uszkodzeniem lub nieuprawnionym zniszczeniem tych danych.
10. Wzór upoważnienia o dopuszczeniu do przetwarzania danych osobowych określa załącznik nr 1 do niniejszej instrukcji.
11. Osoby wyznaczone do przetwarzania danych osobowych w zbiorach i ewidencjach Szkoły lub mogące mieć dostęp do danych osobowych zgromadzonych w ww. zbiorach i ewidencjach podlegają szkoleniu z zakresu prawnej ochrony danych osobowych, a w szczególności z zakresu ustawy o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych oraz procedur wewnętrznych.
12. Osoby, o których mowa w pkt 11, podpisują oświadczenie o zapoznaniu się z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz zachowaniu danych osobowych i sposobu ich zabezpieczenia w tajemnicy. Wzór oświadczenia określa załącznik nr 4. Oświadczenie przechowuje IOD.
13. Szkolenia z zakresu prawnej ochrony danych osobowych przeprowadza IOD lub podmioty zewnętrzne.
14. Decyzję o skierowaniu osoby na szkolenie, o którym mowa w pkt 13, podejmuje bezpośredni przełożony osoby, która realizować będzie zadania związane z przetwarzaniem danych osobowych lub Administrator Danych Osobowych.
15. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do ich ochrony, przetwarzania i udostępniania zgodnie z obowiązującymi przepisami w tym w szczególności RODO, także do nieudostępniania tych danych osobom nieupoważnionym, zabrania ich przez osobę nieuprawnioną oraz zmianą, utratą, uszkodzeniem lub zniszczeniem tych danych.
16. W każdym przypadku naruszenia obowiązujących przepisów w zakresie ochrony, przetwarzania i udostępniania danych osobowych osoba upoważniona do przetwarzania danych zobowiązana jest do niezwłocznego powiadomienia Inspektora Ochrony Danych.
17. Osoby upoważnione do przetwarzania danych osobowych ponoszą odpowiedzialność karną i dyscyplinarną za naruszenie przepisów o ochronie danych osobowych.
18. Cofnięcie upoważnienia do danych osobowych następuje:
    a) W przypadku stwierdzenia nieuprawnionego udostępnienia danych osobowych osobom nieupoważnionym, dopuszczenia do ich zabrania przez osobę nieuprawnioną, przetwarzania z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem z winy osoby posiadającej upoważnienie;
    b) Po zakończeniu pracy (ustaniu czynności) na stanowisku związanym z przetwarzaniem i dostępem do danych osobowych.
19. Cofnięcie upoważnienia następuje na wniosek bezpośredniego przełożonego osoby, która realizuje zadania związane z przetwarzaniem danych osobowych lub IOD.

20. Cofnięcie upoważnienia następuje w formie pisemnej, zgodnie ze wzorem określonym w załączniku nr 2 do niniejszej instrukcji.

U P O W A Ż N I E N I E

Nr……../ ……..

do przetwarzania danych osobowych

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z 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 – RODO), upoważniam:

Pana / Panią ……

(imię i nazwisko, stanowisko służbowe)

do przetwarzania danych osobowych (obsługi systemu informatycznego/nieinformatycznego) zawartych w zbiorze danych osobowych noszącym nazwę:

……

(nazwa zbioru/zbiorów danych osobowych)

prowadzonym w Zespole Szkół nr 1 w Otwocku, w celu:

……

Wyżej wymieniona osoba została przeszkolona, zrozumiała treści ochrony danych osobowych, i dopuszczona jest do przetwarzania jedynie w zakresie określonym w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) z 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 – RODO) i wydanych do niego przepisów wykonawczych i instrukcji w Zespole Szkół nr 1 w Otwocku.

Wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Zespole Szkół nr 1 w Otwocku.

Upoważnienie obejmuje prawo do przetwarzania danych osobowych w zakresie:

……

Upoważnienie jest ważne do: ……..

……., dnia …….. ……

*(podpis, pieczęć)**

** Wykonujący obowiązki Administratora Danych*

COFNIĘCIE UPOWAŻNIENIA

Nr ……/……

do przetwarzania danych osobowych

Na podstawie „Instrukcji nadawania upoważnień do przetwarzania danych osobowych w Zespole Szkół nr 1 w Otwocku, cofam:

Panu/Pani ……

(imię i nazwisko, stanowisko służbowe)

Upoważnienie Nr ……/……

wydane dla celów przetwarzania danych osobowych w zbiorze danych osobowych:

……

(nazwa zbioru/zbiorów danych osobowych)

prowadzonym w Zespole Szkół nr 1 w Otwocku.

Powód cofnięcia: ……..

……..

(podpis i pieczęć bezpośredniego przełożonego osoby)

……, dnia …… ……..

*(podpis, pieczęć)**

**Wykonujący obowiązki Administratora Danych*

EWIDENCJA UPOWAŻNIEŃ

OSÓB UPRAWNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

w Zespole Szkół nr 1 w Otwocku

L.p.	Imię i nazwisko	Nr upoważnienia	Data nadania uprawnień	Okres dostępu	Nazwa zbioru	Podpis ADO lub IOD

** jeżeli dane przetwarzane są w systemie informatycznym*

..... ……., dnia .....

(imię i nazwisko osoby)

……

(nazwa komórki organizacyjnej)

O Ś W I A D C Z E N I E

Ja, niżej podpisana(y), …… oświadczam, że zostałem przeszkolony oraz zapoznała(e)m się z przepisami dotyczącymi przetwarzania i ochrony danych osobowych, zrozumiała(e)m ich treść i zobowiązuję się do ich przestrzegania.

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) z 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 – RODO).
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000).
3. Zapisy dotyczące bezpieczeństwa przetwarzania i ochrony danych osobowych, określone w Polityce Bezpieczeństwa Danych Osobowych Zespołu Szkół nr 1 w Otwocku.

<u>Jednocześnie oświadczam, że:</u>

1. zapewnię ochronę danym osobowym przetwarzanym w Zespole Szkół nr 1 w Otwocku, a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem;
2. zachowam w ścisłej tajemnicy wszelkie informacje techniczne, technologiczne, prawne i organizacyjne dotyczące systemów i sieci informatycznych / teleinformatycznych oraz dane osobowe, uzyskane w trakcie wykonywania umowy niezależnie od formy przekazania tych informacji i ich źródła;
3. będę wykorzystywał uzyskane informacje jedynie w celach określonych ustaleniami umowy oraz wynikających z uregulowań prawnych obowiązujących w Polsce i Unii Europejskiej;
4. natychmiast przekażę Inspektorowi Ochrony Danych stwierdzenie próby lub faktu naruszenia ochrony lub bezpieczeństwa przetwarzanych danych osobowych;
5. jestem również świadomy(a) odpowiedzialności karnej, dyscyplinarnej i służbowej wynikającej z nieprzestrzegania przepisów ustawy o ochronie danych osobowych.

…… ……..

(Podpis przyjmującego oświadczenie) (Nr ewidencyjny i podpis składającego oświadczenie)

Oświadczenie wypełnia osoba, która wykonując swoje obowiązki musi posiadać dostęp do danych osobowych przetwarzanych w Zespole Szkół nr 1 w Otwocku. Oświadczenie jest zgodne z Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000).

PROCEDURA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Niniejsza instrukcja reguluje postępowanie pracowników Szkoły zatrudnionych przy przetwarzaniu danych osobowych, definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie.
2. Celem niniejszej instrukcji jest określenie zadań pracowników w zakresie:
   a) ochrony danych osobowych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem, ujawnieniem lub pozyskaniem, a także ich utratą oraz ochroną zasobów technicznych;
   b) prawidłowego reagowania pracowników zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia ochrony danych osobowych lub zabezpieczeń systemu informatycznego;
   c) ograniczenia ryzyka powstania zagrożeń oraz minimalizacji skutków wystąpienia zagrożeń.
3. Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:
   a) stanu urządzeń technicznych;
   b) zawartości zbiorów danych osobowych;
   c) sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej;
   d) metod pracy (w tym obiegu dokumentów).
4. Każdy pracownik Szkoły, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest niezwłocznie powiadomić IOD lub bezpośredniego przełożonego.
5. Do typowych zagrożeń bezpieczeństwa danych osobowych należą
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   b) niewłaściwe zabezpieczenie sprzętu IT i 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).
6. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);

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).

7. W przypadku stwierdzenia wystąpienia zagrożenia bezpieczeństwa danych, IOD prowadzi postepowanie wyjaśniające, w toku którego:
   a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
   b) inicjuje ewentualne działania dyscyplinarne;
   c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
   d) dokumentuje czynności podjęte w prowadzonym postępowaniu poprzez sporządzenie pisemnego raportu z zagrożenia bezpieczeństwa danych osobowych, podejmuje działania zapobiegawcze.
8. W przypadku stwierdzenia naruszenia bezpieczeństwa danych, IOD prowadzi postępowanie wyjaśniające, w toku którego dokumentuje czynności podjęte w prowadzonym postępowaniu poprzez sporządzenie pisemnego raportu o naruszeniu ochrony danych osobowych według załączonego wzoru, który zawiera co najmniej:
   a) kod formy naruszenia danych osobowych według załączonego katalogu zagrożeń i incydentów bezpieczeństwa danych osobowych (zał. nr 5);
   b) ustala datę, czas, miejsce wystąpienia naruszenia, jego zakres, przyczyny ujawnienia, skutki oraz wielkość szkód, które zaistniały;
   c) zabezpiecza ewentualne dowody winy;
   d) ustala osoby odpowiedzialne za naruszenia;
   e) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
   f) inicjuje działania dyscyplinarne;
   g) rekomenduje działania prewencyjne (korekcyjne, korygujące, zapobiegawcze), zmierzające do eliminacji podobnych zagrożeń w przyszłości.
9. IOD sporządzony raport ewidencjonuje w „Rejestrze incydentów i zagrożeń".

Procedura działań korygujących i zapobiegawczych

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych, wynikających z zaistnienia naruszeń lub zagrożeń bezpieczeństwa danych oraz zagrożeń systemu ochrony danych osobowych.
2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami ustawy o ochronie danych osobowych, jak również na poprawne

funkcjonowanie systemu ochrony danych osobowych.

3. Osobą odpowiedzialną za nadzór nad procedurą jest IOD.
4. Definicje:
    a) incydent – naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;
    b) zagrożenie – potencjalna możliwość wystąpienia incydentu;
    c) korekcja – działanie w celu wyeliminowania skutków incydentu;
    d) działanie korygujące – jest to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;
    e) działanie zapobiegawcze – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej;
    f) kontrola – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki bezpieczeństwa danych osobowych oraz instrukcji zarządzania systemem informatycznym.

Opis czynności

1. IOD jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
    a) zgłoszenia od kierowników komórek organizacyjnych lub pracowników;
    b) wyniki kontroli, w tym ustalone przyczyny i okoliczności naruszenia bezpieczeństwa danych osobowych.
2. W przypadku, gdy IOD stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa:
    a) źródło powstania incydentu lub zagrożenia;
    b) zakres działań korygujących lub zapobiegawczych;
    c) termin realizacji oraz osobę odpowiedzialną.
3. Bezpośredni przełożony pracownika, po stwierdzeniu naruszenia bezpieczeństwa danych osobowych jest zobowiązany niezwłocznie powiadomić IOD, chyba że zrobił to pracownik, który stwierdził naruszenie. Na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych, IOD lub osoba przełożona pracownika przejmują nadzór nad pracą w systemie, odsuwając jednocześnie od stanowiska pracownika, który dotychczas na nim pracował, aż do czasu wydania odmiennej decyzji.
4. IOD zobowiązany jest do powiadomienia o zaistniałej sytuacji ADO, który podejmuje decyzje o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie. IOD zobowiązany jest do

sporządzenia „Raportu z przeglądu incydentów i zdarzeń”, przedstawiając go do zatwierdzenia ADO.

5. IOD lub ADO są zobowiązani do powiadomienia o zaistniałej sytuacji osobę, której dane związane są z incydentem dotyczącym naruszenia lub wyciekiem danych jej dotyczących.

Za naruszanie ochrony danych osobowych obowiązują kary przewidziane przepisami prawa. Za naruszenie ochrony danych osobowych ADO może stosować kary porządkowe, niezależnie od zastosowania kar, o których mowa wyżej.

Katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

Nr (kod) naruszeń	Formy naruszeń	Sposób postępowania	
		Kierownika komórki organizacyjnej	**Inspektora Ochrony Danych**
A. Formy naruszenia danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych			
A.1	**W zakresie wiedzy**		
A.1.1	Ujawnienie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić IOD.	Sporządza raport z opisem, jaka informacja została ujawniona.
A.1.2	Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić IOD.	Sporządza raport z opisem, jaka informacja została ujawniona.
A.1.3	Dopuszczenie i stwarzanie warunków, aby ktokolwiek mógł pozyskać informację o sprzęcie i pozostałej infrastrukturze informatycznej np. z obserwacji lub dokumentacji.	Natychmiast przerwać czynność prowadzącą do ujawnienia informacji. Powiadomić IOD.	Sporządza raport z opisem, jaka informacja została ujawniona.
A.2	**W zakresie sprzętu i oprogramowania**		
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Pouczyć osobę, która dopuściła do takiej sytuacji. Przekazać informacje do IOD.	Przyjmuje informacje od kierownika komórki organizacyjnej i sporządza raport.

A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła się do takiej sytuacji. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
A.2.3	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności widocznym miejscu, zapisanego hasła dostępu do bazy danych osobowych i sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić IOD.	Sporządza raport.
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska pracy. Ustalić, jakie czynności zostały wykonane przez osobę nieuprawnioną Niezwłocznie powiadomić IOD.	Sporządza raport.
A.2.5	Samodzielne instalowanie i wykorzystanie nielegalnego oprogramowania oraz narzędzi służących do obchodzenia zabezpieczeń w systemach informatycznych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Wzywa administratora systemu informatycznego w celu odinstalowania programów. Sporządza raport.
A.2.6	Zmiana konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez niepowołane osoby.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Wzywa administratora systemu informatycznego w celu przywrócenia stanu pierwotnego. Sporządza raport.
A.2.7	Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa	Wzywa administratora systemu informatycznego w celu wykonania kontroli antywirusowej. Sporządza

		pracy.	raport.
A.2.8	Wykorzystanie ogólnodostępnych serwisów pocztowych (np. Wirtualna Polska, Onet.pl, o2.pl) w celach służbowych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
A.2.9	Wykorzystanie służbowej poczty elektronicznej do celów prywatnych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
A.3	**W zakresie dokumentów i obrazów zawierające dane osobowe**		
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Przekazać informację do IOD.	Przyjmuje informację od kierownika komórki organizacyjnej
A.3.2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Spowodować poprawienie zabezpieczeń. Przekazać informacje do IOD.	Przyjmuje raport od kierownika komórki organizacyjnej.
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
A.3.4	Dopuszczenie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. powiadomić IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
A.3.5	Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawniona osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane	Przyjmuje raport od kierownika komórki organizacyjnej.

		– sporządzić raport.	
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić IOD.	Przyjmuje informacje od kierownika jednostki organizacyjnej.
A.3.7	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić IOD.	Przyjmuje informacje raport od kierownika komórki organizacyjnej.
A.4	**W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych**		
A.4.1	Opuszczenie i pozostawienie bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
A.4.2	Wpuszczenie do pomieszczenia osób nieznanych i dopuszczenie ich do kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Zawiadomić IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.

A.4.3	Dopuszczenie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiejkolwiek urządzenia do sieci komputerowej, demontowały elementy obudów do gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
A.4.4	Pozostawienie otwartych okien lub drzwi po zakończeniu pracy.	Zabezpieczyć (zamknąć) pomieszczenie. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
A.4.5	Pożar, zalanie.	Podjąć próbę odzyskania dokumentacji i sprzętu. Powiadomić IOD.	Przyjmuje informacje od kierownika jednostki organizacyjnej.
A.4.6	Nieprzestrzeganie polityki czystego biurka oraz czystego ekranu	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
A.4.7	Pozostawienie dokumentów w koszu na śmieci.	Zabezpieczyć dokumenty. Przekazać informację do IOD.	Przyjmuje informację od kierownika komórki organizacyjnej.
A.4.8	Pozostawienie wydruków na ogólnodostępnej drukarce.	Zabezpieczyć dokumenty. Przekazać informację do IOD.	Przyjmuje informację od kierownika komórki organizacyjnej.
A.4.9	Nieautoryzowane wykonanie kopii klucza do pomieszczeń biurowych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
A.4.10	Wyniesienie kluczy od pomieszczeń biurowych po zakończonej pracy.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie	Sporządza raport.

		powiadomić IOD.	
A.5	**W zakresie pomieszczeń, w których znajdują się komputery centralne i urządzenia sieci.**		
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakiejkolwiek manipulacji przy urządzeniach lub okablowaniach sieci komputerowej w miejscach publicznych (hole, korytarze, itp.)	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD.	Przyjmuje informacje od kierownika komórki organizacyjnej.
A.5.2	Dopuszczenie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD.	Przyjmuje informacje od kierownika komórki organizacyjnej.
B. Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych.			
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
B.2	Obecność nowych kabli o nieznanym przeznaczeniu lub pochodzeniu.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie	Przyjmuje informacje od kierownika komórki

	aplikacji służącej do przetwarzania danych osobowych.	używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	organizacyjnej. Sporządza raport.
B.4	Nieoczekiwane, niedające się wyjaśnić, zmiany zawartości bazy danych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej.
B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie IOD.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
B.7	Zidentyfikowano środek przetwarzający informacje nieznanego pochodzenia (sprzęt, nośnik.)	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
B.8	Wykorzystano niezinwentaryzowany środek przetwarzania informacji (nie będący własnością pracodawcy).	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
B.9	Przechowywanie haseł w niewłaściwy sposób.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Wzywa administratora systemu informatycznego w celu przywrócenia stanu pierwotnego. Sporządza raport

B.10	Przekazywanie haseł innym osobom.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Wzywa administratora systemu informatycznego w celu przywrócenia stanu pierwotnego. Sporządza raport.
B.11	Pojawienie się nieautoryzowanej informacji na stronie internetowej.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej.
B.12	Niewłaściwe niszczenie nośników z danymi pozwalającymi na ich odczyt.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD	Wzywa administratora systemu informatycznego w celu przywrócenia stanu pierwotnego. Sporządza raport.
B.13	Wykorzystanie służbowych środków przetwarzania informacji do celów prywatnych.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji	Sporządza raport.
B.14	Nadmierne uprawnienia w systemach w stosunku do wykonywanej pracy.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
B.15	Nieuprawniona zmiana danych lub ich uszkodzenie.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
B.16	Fizyczne zniszczenie lub uszkodzenie sprzętu oraz nośników przetwarzających informacje.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.

		wyjaśnienia sytuacji.	
B.17	Kradzież sprzętu przetwarzającego informacje.	Niezwłocznie powiadomić IOD oraz służby informatyczne.	Przyjmuje informacje od kierownika komórki organizacyjnej.
B.18	Błędy w obsłudze i konserwacji sprzętu komputerowego służącego do przetwarzania informacji.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
B.19	W wyniku rozwiązania umowy z pracownikiem nie podjęto działań związanych z odebraniem uprawnień.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
B.20	Nieuprawniony dostęp do strefy administracyjnej.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
C. Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem.			
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić IOD.	Przyjmuje informacje od kierownika komórki organizacyjnej.

C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Powiadomić IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
C.3	Niewykonanie kopii zapasowych	Powiadomić IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
C.4	Niezweryfikowanie możliwości odtworzenia danych z kopii zapasowych.	Powiadomić IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.

Raport z incydentu naruszającego bezpieczeństwo danych osobowych ze względu na poufność, dostępność i integralność

Sporządzający raport

Imię i nazwisko	
Stanowisko (funkcja)	
Dział, pokój nr	

Kod formy naruszenia ochrony danych ..... (wg tabeli)

1) Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):

.....
.....

2) Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):

.....
.....

3) Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:

.....
.....

4) Informacje o danych, które zostały lub mogły zostać ujawnione:

.....
.....

5) Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

.....
.....

6) Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania korekcyjne, korygujące, zapobiegawcze):

.....
.....

Data:..... Podpis:

Raport z zagrożenia bezpieczeństwa danych osobowych

Sporządzający raport

Imię i nazwisko	
Stanowisko (funkcja)	
Dział, pokój nr	

Kod formy zagrożenia ochrony danych ..... (wg tabeli)

1) Miejsce, dokładny czas i data stwierdzenia zagrożenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):

.....
.....

2) Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do zagrożenia ochrony danych osobowych):

.....
.....

3) Osoby, które uczestniczyły w zdarzeniu związanym z zagrożeniem ochrony danych osobowych:

.....
.....

4) Informacje o danych, które mogły zostać ujawnione:

.....
.....

5) Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

.....
.....

6) Krótki opis wydarzenia związanego z zagrożeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania zapobiegawcze):

.....
.....

Data:..... Podpis

Rejestr incydentów i zagrożeń

Nr raportu Zagrożenia/ incydentu	Kod formy naruszenia	Osoba		Podjęte działania			Wyniki podjętych działań	Data zamknięcia zagrożenia/ incydentu	Uwagi
		zgłaszająca	Powodująca naruszenie	zapobiegawcze	korygujące	korekcyjne			

Raport z przeglądu zagrożeń/incydentów bezpieczeństwa danych osobowych

RAPORT Z PRZEGLĄDU ZAGROŻEŃ/INCYDENTÓW	Nr przeglądu
	Data sporządzenia raportu
Data przeprowadzenia przeglądu	
Podsumowanie wyników przeglądu: …… …… …… …… ……	
Spostrzeżenia służące doskonaleniu: …… …… …… …… …… …… …… …… ……	
Załączniki do raportu:	

…… ……

Sporządził Zatwierdził

Procedura postępowania w przypadku wystąpienia wniosku informacyjnego od osoby, której dane dotyczą.

1. Zgodnie z art. 13 i art. 15 RODO, na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany poinformować o przysługujących jej prawach oraz udzielić, odnośnie jej danych osobowych, informacji dotyczących:

   a. celu przetwarzania danych;
   b. odbiorców lub kategorii odbiorców, którym dane zostały lub zostaną ujawnione;
   c. planowanego okresu przetwarzania danych;
   d. praw przysługujących osobie, której dane dotyczą (w szczególności prawo do poprawienia, usunięcia, ograniczenia przetwarzania danych, wniesienia sprzeciwu do organu nadzorującego);
   e. zautomatyzowanego podejmowania decyzji w oparciu o zebrane dane i jego konsekwencjach;
   f. źródła danych.

2. Administrator obowiązany jest udzielić informacji wymienionych w pkt 1 w terminie 30 dni od otrzymania wniosku. Termin ten może zostać przedłużony o kolejne 2 miesiące z uwagi na skomplikowany charakter wniosku lub dużą ilość wniosków. Przedłużenie terminu następuje po uprzednim poinformowaniu wnioskodawcy o przyczynach opóźnienia.

3. Na wniosek osoby zainteresowanej wymienionych informacji udziela się na piśmie.

4. Osoba, której dane dotyczą ma prawo do wielokrotnego zgłaszania wniosku o udzielenie ww. informacji, pod warunkiem, że zgłoszenia te następują w racjonalnych odstępach czasu.

5. Administrator danych może odmówić udzielenia informacji wymienionych w pkt 1 osobie, której dane dotyczą, gdy udostępnienie informacji spowodowałoby:

   a. ujawnienie wiadomości zawierających informacje niejawne;
   b. zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego;
   c. zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa;
   d. istotne naruszenie dób osobistych osób, których dane dotyczą lub innych osób.

6. Administrator może również odmówić podjęcia działań, jeżeli wniosek o udzielenie informacji jest nieuzasadniony lub nadmierny (zbyt częsty). Na administratorze spoczywa ciężar udowodnienia braku uzasadnienia lub nadmierności wniosku. O decyzji dotyczącej

niepodjęcia działań administrator musi poinformować wnioskodawcę niezwłocznie, nie później niż w terminie 1 miesiąca od otrzymania wniosku. Administrator podaje w decyzji przyczyny niepodjęcia działań oraz informuje o możliwości wniesienia skargi do odpowiedniego organu nadzoru.

7. W przypadku uzasadnionej wątpliwości administratora dotyczącej tożsamości wnioskodawcy, administrator może żądać od wnioskodawcy dodatkowych informacji, w celu potwierdzenia jego tożsamości.

8. Administrator udziela informacji wymienionych w pkt 1 nieodpłatnie.

Procedura postępowania w przypadku złożenia sprzeciwu co do przetwarzania danych osobowych do celów marketingu bezpośredniego.

1. Na podstawie art. 21 RODO, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów.

2. Sprzeciw można wnieść, jeśli administrator twierdzi, że wykorzystuje dane osobowe w oparciu o:

   a. przesłankę dopuszczalności przetwarzania danych wymienioną w art. 6 ust. 1 lit. e) rozporządzenia (przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi);

   b. przesłankę wymienioną w art. 6 ust. 1 lit. f) rozporządzenia (przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem);

tymczasem zaś zamierza je przetwarzać w celach marketingowych lub przekazać je innemu administratorowi danych.

3. Prawo sprzeciwu nie przysługuje osobie, której dane dotyczą, gdy podstawą przetwarzania danych jest zgoda tej osoby, realizacja obowiązku lub uprawnienia wynikającego z przepisu prawa albo gdy przetwarzanie danych służy zawarciu lub wykonaniu umowy między administratorem a osobą, której dane dotyczą.

4. Wniesienie sprzeciwu przez osobę, której dane dotyczą, oznacza konieczność zaprzestania wykorzystywania jej danych osobowych.

5. W razie wniesienia sprzeciwu dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Możliwe jest jednak pozostawienie w zbiorze imienia i nazwiska osoby oraz numeru PESEL albo adresu – wyłącznie dla uniknięcia ponownego wykorzystania danych osoby w celach objętych sprzeciwem.

Klauzula obowiązku informacyjnego dla Zespołu Szkół nr 1 w Otwocku

Zgodnie z art. 13 i 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 – RODO), informujemy, że:

1. Administratorem Danych Osobowych jest Zespół Szkół nr 1 w Otwocku, z siedzibą przy ul. Słowackiego 4/10, 05 – 400 Otwock.

2. Inspektorem Ochrony Danych jest Paweł Maliszewski (iod@perfectinfo.pl).

3. Dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c Rozporządzenia, w celu realizacji ustawowych i statutowych zadań Szkoły i nie będą udostępniane podmiotom innym, niż upoważnione na podstawie przepisów prawa.

4. Odbiorcami danych osobowych są Pracownicy Zespołu Szkół nr 1 w Otwocku.

5. Dane osobowe przetwarzane będą w okresie niezbędnym do realizacji Państwa obsługi oraz w zgodzie z wymogami prawa.

6. Posiadają Państwo prawo dostępu do treści swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych.

7. Jeżeli przetwarzanie danych osobowych odbywa się na podstawie zgody, posiadają Państwo prawo do jej cofnięcia w dowolnym momencie, bez wpływu na zgodność w prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

8. W przypadku stwierdzenia, że dane osobowe nie są przetwarzane zgodnie z wymogami Rozporządzenia, posiadają Państwo prawo wniesienia skargi do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych.

9. Podanie danych osobowych jest dobrowolne, jednakże w przypadku ich niepodania nie będziemy w stanie świadczyć Państwu usług.

10. Nie podlegają Państwo zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.