Załącznik Nr 1 do Zarządzenia z dnia 25 maja 2018 r.

Polityka ochrony danych osobowych

przetwarzanych w Niepublicznej Szkole Podstawowej im. „Akcji III Most” w Przybysławicach

SPIS TREŚCI

I. Wstęp

1. W dążeniu do zapewnienia wysokiego poziomu ochrony przetwarzanych danych osobowych, w tym zabezpieczenia danych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w Niepublicznej Szkole Podstawowej im. „Akcji III Most" w Przybysławicach określa się „Politykę ochrony danych osobowych przetwarzanych w Niepublicznej Szkole Podstawowej im. „Akcji III Most" w Przybysławicach"
2. Dyrektor Niepublicznej Szkoły Podstawowej im. „Akcji III Most" w Przybysławicach Pan Tadeusz Seremet jako Administrator, zobowiązany jest do zabezpieczenia przetwarzanych danych osobowych, poprzez podjęcie środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia praw lub wolności osób fizycznych, z uwzględnieniem wiedzy technicznej, kosztów wdrożenia oraz charakteru, zakresu, kontekstu i celów przetwarzania.
3. Przetwarzanie danych osobowych, może być realizowane po spełnieniu jednego z warunków określonych w art. 6 RODO.
4. Niniejsza polityka ochrony obejmuje wszystkie procesy i czynności przetwarzania danych osobowych w Szkole i odnosi się do zabezpieczenia danych osobowych przetwarzanych zarówno w formie papierowej jak i przy wykorzystaniu systemów teleinformatycznych.

II. Podstawowe pojęcia

Ilekroć w niniejszym dokumencie jest mowa o:

1) Szkole – rozumie się przez to Niepubliczną Szkołę Podstawową im. „Akcji III Most" w Przybysławicach;
2) Administratorze – rozumie się przez to Pan Tadeusz Seremet – dyrektor szkoły;
3) RODO – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE L 119, s. 1);
4) Polityce – rozumie się przez to „Politykę ochrony danych osobowych przetwarzanych w Niepublicznej Szkole Podstawowej im. „Akcji III Most" w Przybysławicach ";
5) ASI – rozumie się przez to administratora systemu informatycznego, czyli pracownika wyznaczonego przez Administratora, odpowiedzialnego za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie;
6) danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
7) przetwarzaniu danych osobowych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie,

rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

III. Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

1. Za bezpieczeństwo danych osobowych przetwarzanych w Szkole odpowiada Administrator, który w myśl przepisów RODO, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
2. Do zadań Administratora należy:
   1) wydawanie upoważnień do przetwarzania danych osobowych – wzór upoważnienia określa **załącznik nr 1**;
   2) odwoływanie upoważnień do przetwarzania danych osobowych – wzór odwołania upoważnienia określa **załącznik nr 2**;
   3) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych – wzór ewidencji określa **załącznik nr 3,**
   4) ewidencjonowanie oświadczeń osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa **załącznik nr 4**,
   5) określanie potrzeb w zakresie stosowanych w Szkole zabezpieczeń, zatwierdzanie rozwiązań i nadzorowanie prawidłowości ich wdrożenia,
   6) podnoszenie świadomości i kwalifikacji osób przetwarzających dane osobowe w Szkole i zapewnienie odpowiedniego poziomu przeszkolenia w tym zakresie,

   Administrator, może wyznaczyć pracownika administracyjnego, który będzie dbał o dokumentację i będzie podlegał Administratorowi.
3. Do zadań ASI należy:
   1) zarządzanie bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami Administratora,
   2) doskonalenie metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
   3) przydzielanie identyfikatorów użytkownikom systemu informatycznego oraz zaznajamianie ich z procedurami ustalania i zmiany haseł dostępu,
   4) nadzorowanie prac związanych z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
   5) zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
   6) prowadzenie nadzoru nad archiwizacją zbiorów danych oraz zabezpieczanie elektronicznych nośników informacji zawierających dane osobowe.
4. Pracownik upoważniony do przetwarzania danych osobowych:
   1) chroni prawo do prywatności osób fizycznych powierzających Szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce;
   2) zapoznaje się zasadami określonymi w Polityce i składa oświadczenie o znajomości tych przepisów;

3) za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą ponosi odpowiedzialność karną, wynikająca z przepisów ustawy o ochronie danych osobowych lub pracowniczą na zasadach określonych w kodeksie pracy.

IV. Realizacja praw osób, których dane są przetwarzane w Szkole

1. W Szkole wprowadza się rozwiązania, które pozwalają na realizowanie praw osób, których dane są przetwarzane. W szczególności dotyczy to:
   1) umożliwienia osobom, których dane dotyczą wyrażenia zgody na przetwarzanie danych osobowych (gdy brak innej podstawy do przetwarzania danych),
   2) informowania osób, których dane dotyczą o zbieraniu i przetwarzaniu tych danych,
   3) prawa dostępu przysługującego osobom, których dane dotyczą,
   4) prawa osób, których dane dotyczą, do sprostowania danych,
   5) prawa osób, których dane dotyczą, do usunięcia swoich danych („prawa do bycia zapomnianym”),
   6) prawa osób, których dane dotyczą, do ograniczenia przetwarzania danych.
2. Spełnienie obowiązków informacyjnych względem osób, których dane są przetwarzane odbywa się poprzez przekazanie osobom wymaganych prawem informacji przy zbieraniu danych oraz udokumentowanie realizacji tych obowiązków.
3. Warunkiem prawidłowego spełnienia obowiązku informacyjnego wobec osoby, której dane dotyczą, jest przekazanie jej w zwięzłej, przejrzystej i zrozumiałej formie, jasnym i prostym językiem wszelkich informacji, o których mowa w art. 13 i 14 RODO oraz prowadzenie z nią wszelkiej korespondencji, w myśl art. 15-22 i 34 RODO w sprawie przetwarzania danych osobowych.
4. Informacji, o których mowa w pkt. 3 udziela się na piśmie, w tym w stosownych przypadkach – elektronicznie lub w inny sposób (np. ustnie).
5. Informacje podawane na mocy art. 13 i 14 RODO oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 RODO są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nadmierne, w szczególności ze względu na swój ustawiczny charakter, Szkoła może pobrać opłatę uwzględniającą administracyjne koszty udzielenia informacji.
6. Realizacja zadań, o których mowa w pkt. 1 uwzględnia zasady, w tym wyłączenia, które zostały określone w obowiązujących przepisach prawa o ochronie danych osobowych.
7. Dostęp, usunięcie lub ograniczenie przetwarzania danych osobowych musi być zgodne z przepisami prawa, na podstawie których odbywa się przetwarzanie oraz na podstawie przepisów prawa określających zasady przetwarzania dokumentacji archiwalnej.

V. Powierzenie przetwarzania danych osobowych

1. Przetwarzanie powierzonych danych może być realizowane wyłącznie przez podmioty, które gwarantują odpowiednie środki techniczne i organizacyjne dające możliwość spełnienia wymogów RODO, w tym w szczególności skutecznie chroniło prawa osób, których dane dotyczą.

2. Przy określaniu minimalnych wymogów, które powinien spełnić podmiot przetwarzający należy brać pod uwagę charakter, skalę i zakres przetwarzania oraz, jeśli to konieczne, uwzględniać wyniki szacowania ryzyka przeprowadzone w Szkole w tym zakresie.
3. Powierzenie przetwarzania danych osobowych odbywa się na podstawie pisemnej umowy lub porozumienia, które wyraźnie określają charakter i cel przetwarzania, przedmiot i czas trwania przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, oraz obowiązki i prawa administratora i podmiotu przetwarzającego.
4. Dokumentacja, na podstawie której następuje powierzenie danych, musi mieć formę pisemną (dopuszcza się prowadzenie tej dokumentacji w formie elektronicznej).
5. Dokumentacja, na podstawie której następuje powierzenie danych, musi gwarantować Administratorowi realizację zadań wynikających z zapisów art. 28 RODO, w tym w szczególności:
   1) możliwość egzekwowania wskazanych w dokumentacji obowiązków podmiotu przetwarzającego,
   2) możliwość przeprowadzanie kontroli/audytów w zakresie realizacji umowy powierzenia,
   3) możliwości weryfikacji czy powierzone dane nie zostały przekazane innemu podmiotowi przez przetwarzającego bez zgody („podpowierzenie danych").

VI. Udostępnianie danych osobowych

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia Administratora danych osobowych może mieć miejsce wyłącznie w przypadku działań osób i podmiotów uprawnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
2. Dane osobowe mogą być udostępniane:
   1) podmiotom i organom publicznym działającym w granicach przyznanych im uprawnień, po okazaniu dokumentów potwierdzających te uprawnienia;
   2) stronom postępowań administracyjnych prowadzonych w Szkole, na zasadach określonych w kodeksie postępowania administracyjnego lub odrębnych przepisów.
3. Administrator odmawia udostępnienia danych osobowych jeżeli spowodowałoby to naruszenie przepisów prawa.

VII. Analiza ryzyka

1. W trakcie procesu zarządzania ryzykiem przeprowadzana jest identyfikacja zagrożeń bezpieczeństwa danych osobowych oraz określane są podatności i skutki wystąpienia tych zagrożeń oraz kategoryzacja danych i czynności przetwarzania pod kątem ryzyka, które przedstawiają.
2. W ramach procesu zarządzania ryzykiem przeprowadzana jest:
   1) analiza ryzyka dla czynności przetwarzania danych lub ich kategorii;
   2) ocena skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie.

3. Uzyskane, w ramach procesu analizy ryzyka, wyniki są podstawą do dalszego postępowania ze zidentyfikowanymi ryzykami w kontekście wdrożenia rozwiązań technicznych i organizacyjnych, które pozwolą ochronić dane osobowe przed utratą ich podstawowych atrybutów (poufności, integralności, dostępności, rozliczalności) oraz pozwolą zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania tych danych w Szkole.
4. Ocena skutków czynności przetwarzania dla ochrony danych oraz ich wpływu na naruszenia praw lub wolności osób fizycznych obejmuje analizę i rozpatrywanie możliwych sytuacji i scenariuszy naruszenia ochrony danych osobowych przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania, oraz różnego prawdopodobieństwa wystąpienia i wagi zagrożenia.
5. W ramach przeprowadzanej oceny, o której mowa w pkt. 4, należy brać pod uwagę wskazane przez Prezesa UODO rodzaje procesów i czynności przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych.

VIII. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

Szkoła nie przekazuje danych osobowych do państw trzecich lub organizacji międzynarodowych.

IX. Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

1. Pomieszczenia, w których przetwarzane są dane osobowe, pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia musi być poprzedzone przeniesieniem danych osobowych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.
2. Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych, w zakresie zgodnym z kategorią danych.
3. Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z Administratorem, w przypadku pracowników upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

X. Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w Instrukcji zarządzania systemem informatycznym, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego Szkoły, stanowiącej **załącznik nr 5.**

XI. Naruszenie bezpieczeństwa danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych w Szkole jest zobowiązana do natychmiastowego powiadamiania Administratora o wystąpieniu incydentu związanego z naruszeniem ochrony danych osobowych.
2. Szczegółowy tryb postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych, został określony w **załączniku nr 6.**

XII. Weryfikacja systemu ochrony danych

1. Weryfikacja systemu ochrony danych odbywa się poprzez prowadzenie kontroli okresowych nie rzadziej niż raz w roku.
2. W zależności od potrzeb, część prac w ramach weryfikacji systemu ochrony danych, może zostać zlecone podmiotowi zewnętrznemu.

XIII. Postanowienia końcowe

1. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszym dokumencie oraz pozostałej dokumentacji, która uszczegóławia wymagania i zasady ochrony danych osobowych.
2. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako naruszenie obowiązków służbowych.
3. Polityka oraz pozostała dokumentacja, która uszczegóławia wymagania i zasady ochrony danych osobowych może być udostępniania osobom trzecim, jeżeli nie zawiera w swojej treści i w załącznikach szczegółowych informacji o wdrożonych w Szkole zabezpieczeniach danych osobowych oraz innych informacji prawnie chronionych.

XIV. Wykaz załączników

Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych

Załącznik nr 2 – Odwołanie upoważnienia

Załącznik nr 3 – Ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 4 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych

Załącznik nr 5 – Instrukcja zarządzania systemem informatycznym

Załącznik nr 6 – Zasady postępowania w przypadku wykrycia naruszenia ochrony danych osobowych przetwarzanych w Niepublicznej Szkole Podstawowej im. „Akcji III Most” w Przybysławicach .

Załącznik Nr 1 do Polityki

……., dnia ……..... r.

.....
(pieczęć Szkoły)

UPOWAŻNIENIE nr ……/20…..
do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE L 119, s. 1)

upoważniam Panią/Pana .....

zatrudnioną (ego) w ……. do przetwarzania danych osobowych zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w zakresie wynikającym z zajmowanego stanowiska pracy, w okresie

od dnia ..... 20…. r. do ……

Informuję, że Pani/Pan została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Szkole.

.....
(podpis Administratora)

Przyjmuję do wiadomości i stosowania.

…….....
(Podpis osoby upoważnionej)

Załącznik Nr 2 do Polityki

……, dnia ……..... r.

.....
(pieczęć Szkoły)

ODWOŁANIE UPOWAŻNIENIA nr …
do przetwarzania danych osobowych

Odwołuję z dniem …….. upoważnienie nr ……/20…. do przetwarzania danych osobowych wystawione dla Pani/Pana ……

Administrator

……..……
(pieczątka i podpis)

Załącznik Nr 3 do Polityki

……., dnia ……..... r.

.....
(pieczęć Szkoły)

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr upoważnienia	Imię i nazwisko	Identyfikator użytkownika *	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data odebrania uprawnień	Uwagi

* Wypełnia się tylko dla osób upoważnionych do przetwarzania danych osobowych, które zostały dopuszczone do przetwarzania danych osobowych w systemie

Załącznik Nr 4 do Polityki

..... ……., dnia ……..... r.
(imię i nazwisko)

.....
(stanowisko)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Szkole zasadach dotyczących przetwarzania danych osobowych, określonych w „Polityce ochrony danych osobowych przetwarzanych w Niepublicznej Szkole Podstawowej im. „Akcji III Most" w Przybysławicach" i zobowiązuję się ich przestrzegać. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w Niepublicznej Szkole Podstawowej im. „Akcji III Most" w Przybysławicach.

Zostałem/am zapoznany/a z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE L 119, s. 1) i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Poinformowano mnie również o grożącej, stosownie do przepisów rozdziału 8 ustawy o ochronie danych osobowych odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, ze złamanie zasad ochrony danych osobowych, obowiązujących w Niepublicznej Szkole Podstawowej im. „Akcji III Most" w Przybysławicach może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

.....
(podpis pracownika)

Załącznik Nr 5 do Polityki

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

I. Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w Szkole.
2. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ASI.
3. ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez Administratora.
4. Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.
5. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

II. Zabezpieczenie danych w systemie informatycznym

1. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system.
2. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.
3. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
   a) rozpoczęcie i zakończenie pracy przez użytkownika systemu,
   b) operacje wykonywane na przetwarzanych danych,
   c) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
   d) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
   e) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
4. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:
   a) identyfikatora osoby, której dane dotyczą,
   b) osoby przesyłającej dane,
   c) odbiorcy danych,
   d) zakresu przekazanych danych osobowych,
   e) daty operacji,
   f) sposobu przekazania danych.
5. Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania”) na każdym komputerze, na którym przetwarzane są dane osobowe.

6. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

III. Zasady bezpieczeństwa podczas pracy w systemie informatycznym

1. W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
   1) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła (autoryzacja użytkownika w bazie usług katalogowych),
   2) loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.
2. W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z sytemu lub uruchomienie wygaszacza ekranu chronionego hasłem.
3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.
5. Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone poinformowaniem pracowników Szkoły przez ASI na co najmniej 30 minut przed planowanym zawieszeniem.
6. Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ASI w razie:
   a) podejrzenia naruszenia bezpieczeństwa systemu;
   b) braku możliwości zalogowania się użytkownika na jego konto;
   c) stwierdzenia fizycznej ingerencji w przetwarzana dane;
   d) stwierdzenia użytkowania narzędzia programowego lub sprzętowego.
7. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:
   a) nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem);
   b) wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach);
   c) różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych);
   d) inne nadzwyczajne sytuacje.

IV. Tworzenie kopii zapasowych

1. Pełne kopie zapasowe zbiorów danych tworzone są 4 razy w ciągu roku. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.
2. Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane.
3. Kopie przechowywane są w szafie metalowej w sekretariacie Szkoły.
4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ASI.

5. Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

V. Przeglądy i konserwacje systemów

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych przedstawicieli wykonawców.
2. Prace wymienione w pkt 1 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3. Przed rozpoczęciem prac wymienionych w pkt 1 przez osoby niebędące pracownikami Szkoły należy dokonać potwierdzenia tożsamości tychże osób.

VI. Niszczenie wydruków i nośników danych

1. Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek / w sposób uniemożliwiający ich odczytanie (pocięte w poprzeczne paski).
2. Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

Załącznik Nr 6 do Polityki

Zasady

postępowania w przypadku wykrycia naruszenia ochrony danych osobowych przetwarzanych w Niepublicznej Szkole Podstawowej im. „Akcji III Most" w Przybysławicach

1. Cel

W niniejszym dokumencie ustalone zostały zasady analizowania przypadków dotyczących naruszenia ochrony danych osobowych oraz sposób postępowania przy zgłaszaniu naruszenia ochrony danych osobowych w myśl przepisów art. 33 i art. 34 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 (Dz. Urz. UE L 119/1, z 4 maja 2016 r.).

2. Definicje

Ilekroć w niniejszej instrukcji zostanie użyte pojęcie:

1) Szkoła – należy przez to rozumieć Niepubliczną Szkołę Podstawową im. „Akcji III Most" w Przybysławicach
2) Administrator – rozumie się przez to Pan Tadeusz Seremet – dyrektor szkoły;
3) RODO – należy przez to rozumieć 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 (Dz. Urz. UE L 119/1, z 4 maja 2016 r.);
4) dane osobowe – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) naruszenie ochrony danych osobowych – należy przez to rozumieć, każdą sytuację która jest wynikiem zdarzeń losowych lub działania sił natury bądź nieumyślnego lub celowego działania człowieka i powoduje lub może spowodować zagrożenie bezpieczeństwa danych osobowych przetwarzanych w Szkole;

3. Zakres stosowania

Instrukcja obowiązuje wszystkich pracowników Szkoły i dotyczy zidentyfikowanych przypadków zagrażających bezpieczeństwu danych osobowych przetwarzanych w Szkole, zarówno w formie papierowej, jaki i przy wykorzystaniu systemów teleinformatycznych.

4. Odpowiedzialność

1) Każda osoba zatrudniona w Szkole lub wykonująca prace na rzecz Szkoły (stażysta, praktykant, przedstawiciel podmiotu zewnętrznego współpracujący ze Szkołą) jest

zobowiązana do niezwłocznego zgłoszenia faktu wykrycia przypadków mających znaczenie dla prawidłowego funkcjonowania Szkoły.

2) Punkt kontaktowy do zgłaszania przypadków związanych z naruszeniem bezpieczeństwa danych osobowych:
- gabinet dyrektora szkoły, pokój nr 19
- tel. 146283464
- adres e-mail: przybyslawice.szkola@op.pl

5. Tryb postępowania

5.1. Wykrycie sytuacji naruszenia bezpieczeństwa danych osobowych.

1) Sytuacje, które będą związane z naruszeniem bezpieczeństwa danych osobowych odnoszą się do:
- utraty danych (kradzież, zgubienie, zniszczenie danych),
- przekazania danych osobie lub podmiotowi nieuprawnionemu na skutek działania umyślnego lub w wyniku błędu pracowników lub współpracowników Szkoły.

2) W przypadku wykrycia naruszenia bezpieczeństwa danych osobowych należy, o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, oraz uwzględnić w działaniu również ustalenie przyczyn lub sprawców. W szczególności należy:
- rozważyć wstrzymanie bieżącej pracy w celu zabezpieczenia miejsca zdarzenia (wylogować się z systemu, wyłączyć urządzenie);
- zaniechać, o ile to możliwe, dalszych działań, które wiążą się z zaistniałą sytuacją i mogą utrudnić jej udokumentowanie i późniejszą analizę;
- w zależności od okoliczności zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałej sytuacji (np. zasady BHP, ewakuacja z budynku, procedury ppoż.),
- poinformować Administratora wg zasad określonych w niniejszym dokumencie.

5.2. Zgłaszanie sytuacji naruszenia bezpieczeństwa danych osobowych.

1) Z uwagi na wymogi wynikające z RODO, w tym krótki okres na zgłoszenie naruszenia bezpieczeństwa danych osobowych (72 godziny od stwierdzenia/wykrycia naruszenia) informacje w tym zakresie muszą być przekazywane przez osoby, które zidentyfikowały zagrożenie, bez zbędnej zwłoki.
2) Wykrycia naruszenia lub podejrzenie wystąpienia zdarzenia, które może mieć wpływ na bezpieczeństwo przetwarzanych danych należy zgłosić do Administratora.
3) Zgłoszenie musi zawierać miejsce wystąpienia naruszenia bezpieczeństwa danych osobowych oraz, w miarę możliwości, jego krótki opis.

5.3. Analiza przypadków naruszenia bezpieczeństwa danych osobowych.

1) Każdy zgłoszony przypadek musi zostać poddany analizie, w zakresie ustalenia czy faktycznie doszło do naruszenia bezpieczeństwa danych osobowych, a w szczególności analiza powinna dać możliwość ustalenia czy doszło do naruszenia bezpieczeństwa danych osobowych, które może skutkować ryzykiem naruszenia praw i wolności osób, np. jeśli naruszenie może prowadzić do kradzieży lub fałszowania tożsamości, straty

finansowej, naruszenia dobrego imienia czy też naruszenia tajemnic prawnie chronionych.

2) W trakcie analizy należy brać pod uwagę następujące elementy:

- wdrożone zabezpieczenia i ich funkcjonowanie (potwierdzenie ich skuteczności),
- zapisy (logi systemowe/rejestry) systemu teleinformatycznego, jeśli zachodzi podejrzenie utraty poufności przetwarzanych danych (np. kradzież danych z bazy),
- poprawność funkcjonowania systemu – bazy danych jeśli zachodzi podejrzenie utraty integralności przetwarzanych danych (np. uszkodzenie bazy danych),
- zapisy (logi systemowe/nagrania/rejestry) systemów zabezpieczeń wspomagających ochronę systemów teleinformatycznych oraz przetwarzanych danych, jeśli zachodzi podejrzenie nieautoryzowanego dostępu do danych.

3) Analiza przeprowadzana jest przez Administratora.

4) O wystąpieniu sytuacji naruszenia bezpieczeństwa danych osobowych przetwarzanych w Szkole jest informowany Administrator.

5.4. Zawiadomienie organu nadzorczego o sytuacji naruszenia bezpieczeństwa danych osobowych.

1) Jeżeli przeprowadzona analiza, o której mowa w podrozdziale 5.3 wskazuje na naruszenie bezpieczeństwa danych osobowych, które może skutkować ryzykiem naruszenia praw i wolności osób, informacja o tym zdarzeniu jest kierowana do Urzędu Ochrony Danych Osobowych.

2) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonywane jest w sposób określony przez organ nadzorczy nie później niż 72 godziny od stwierdzenia (wykrycia) zdarzenia.

3) Jeżeli zgłoszenie naruszenia bezpieczeństwa danych osobowych dokonane zostanie po upływie 72 godzin od stwierdzenia (wykrycia) zdarzenia, musi ono zwierać wyjaśnienie przyczyn opóźnienia.

4) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonuje Administrator.

5.5. Zawiadomienie osoby której dane dotyczą o sytuacji naruszenia bezpieczeństwa jej danych osobowych.

1) Jeżeli przeprowadzona analiza, o której mowa w podrozdziale 5.3 wskazuje na naruszenie bezpieczeństwa danych osobowych, które może skutkować wysokim ryzykiem naruszenia praw i wolności osób, informacja o tym zdarzeniu jest kierowana bez zbędnej zwłoki do osób których dane dotyczą.

2) Zawiadomienia o naruszeniu, powinno zawierać opis jego charakteru naruszenia, możliwe konsekwencje dla osób których dane dotyczą oraz możliwe do zastosowania środki zalecane w celu poradzenia sobie z naruszeniem i zminimalizowania jego negatywnych skutków.

3) Zawiadomienia o naruszeniu powinno zostać przekazane zainteresowanym osobom, biorąc pod uwagę dostępne kanały komunikacji z nimi oraz koszty wysyłki korespondencji np. z uwagi na liczbę osób objętych zawiadomieniem:

- na adres e-mail (jeśli znany),
- telefonicznie (jeśli znany nr telefonu),
- listownie (jeśli znany adres).

4) Zawiadomienie w formie, o której mowa w pkt 2, nie jest wymagane, jeśli:
- w celu zabezpieczenia danych wprowadzone zostały w Szkole rozwiązania uniemożliwiające odczyt osobom nieuprawnionym dostępu do tych danych (np. zaszyfrowanie danych),
- zostały wprowadzone środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osób.

5) Bezpośrednie zawiadomienie nie jest również wymagane, jeśli podawałoby to poniesienie niewspółmiernie dużych nakładów pracy i środków finansowych ze strony Szkoły.
6) W przypadku zaistnienia sytuacji, o której mowa w pkt 5, należy wydać publiczny komunikat (jednorazowe ogłoszenie w dzienniku o zasięgu regionalnym).

5.6. Usuwanie naruszenia bezpieczeństwa danych osobowych

1) W usuwanie naruszenia bezpieczeństwa danych osobowych zaangażowani są pracownicy Szkoły, którzy w ramach powierzonych obowiązków zapewniają i nadzorują funkcjonowanie systemu zabezpieczeń danych osobowych.
2) Po wykryciu naruszenia bezpieczeństwa danych osobowych analizowane są okoliczności związane z jego wystąpieniem oraz ustalany jest sposób rozwiązania problemu oraz, jeśli to konieczne, zabezpieczeniu materiału dowodowego.
3) W przypadku gdy problem może zostać rozwiązany samodzielnie przez pracowników Szkoły, należy to wykonać bez zbędnej zwłoki.
4) W przypadku konieczności wykonania działań przez podmiot zewnętrzny, pracownik zajmujący się rozwiązaniem problemu powinien, używając ustalonych metod, poinformować o zdarzeniu ten podmiot, oraz razem z jej przedstawicielem uczestniczyć w rozwiązywaniu problemu.
5) W przypadku wykrycia działań umyślnych pracownik odpowiedzialny za obsługę naruszenia bezpieczeństwa danych osobowych przekazuje wyniki analizy, wraz z zabezpieczonym materiałem dowodowym, Administratorowi w celu wyciągnięcia konsekwencji dyscyplinarnych wobec pracownika Szkoły lub podjęcia kroków prawych wobec osób trzecich.
6) Po przywróceniu prawidłowego stanu bezpieczeństwa danych osobowych należy przeprowadzić analizę w celu określenia przyczyny naruszenia oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
7) Jeżeli przyczyną naruszenia bezpieczeństwa danych osobowych:
- był błąd osoby przetwarzającej dane, w szczególności użytkownika systemu teleinformatycznego, można przeprowadzić dodatkowe szkolenie lub przesłać stosowną informację do wszystkich użytkowników systemu o sposobie postępowania przy przetwarzaniu danych osobowych oraz zapewnieniu ich bezpieczeństwa;
- było uaktywnienie złośliwego kodu, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe;
- było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje służbowe;
- było włamanie lub uszkodzenie systemu zabezpieczeń w celu pozyskania danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony danych osobowych;

- był zły stan urządzeń lub sposób działania oprogramowania, należy niezwłocznie przeprowadzić kontrolne czynności serwisowe.

8) Do celów dowodowych, naruszenie bezpieczeństwa danych osobowych może zostać dodatkowo szczegółowo udokumentowane.

6. Załączniki

Załącznik nr 1. Wzór „Raportu o naruszeniu danych osobowych”

Załącznik nr 2. Wzór „Zawiadomienia o naruszeniu danych przesyłanego do osób których dane zostały naruszone”

Załącznik nr 1

do „Zasad postępowania w przypadku wykrycia naruszenia ochrony danych osobowych przetwarzanych w Niepublicznej Szkole Podstawowej im. „Akcji III Most” w Przybysławicach”.

Wzór „Raportu o naruszeniu danych osobowych”

1. **Opis naruszenia ochrony danych osobowych**

W dniu …….. zidentyfikowano naruszenie ochrony danych osobowych w zakresie ujawnienia (wskazać rodzaj danych osobowych):

- ……

- ……

- ……

2. **Kategoria i przybliżona liczba osób/wpisów danych których dotyczy naruszenie**

……
……
……

3. **Możliwe konsekwencje naruszenia ochrony danych osobowych**

……
……
……

4. **Opis środków zastosowanych lub proponowanych do zastosowania w celu zaradzenia naruszeniu ochrony danych osobowych**

……
……
……

……

podpis Administratora

Załącznik nr 2

do „Zasad postępowania w przypadku wykrycia naruszenia ochrony danych osobowych przetwarzanych w Niepublicznej Szkole Podstawowej im. „Akcji III Most” w Przybysławicach”.

Wzór „Zawiadomienia o naruszeniu danych osobowych”

Informuję, że w wyniku …… w dniu ……..…. doszło do naruszenia Pani/Pana danych osobowych w zakresie ujawnienia (wskazać rodzaj danych osobowych):

- ……

- ……

- ……

Naruszenie zostało spowodowane (włamaniem i kradzieżą danych z bazy ……../ nieprawidłowym przesłaniem danych przez pracownika/)

W związku z powyższym istnieje duże ryzyko kradzieży lub sfałszowania Pani/Pana tożsamości, co może spowodować stratę finansową lub utratę dobrego imienia w przypadku wykorzystania tych danych przez osoby nieuprawnione w sposób niezgodny z prawem.

Informacja dotycząca kradzieży danych została zgłoszona do organów ścigania

W celu zminimalizowania negatywnych skutków tego naruszenia należy zastrzec dowód tożsamości/zmienić hasło/……

Dodatkowe informacje w tym zakresie można uzyskać:

- pod nr telefonu ……..

- wysyłając zapytanie na adres e-mail: ……..

……

podpis Administratora

I. Osoby zatrudnione w oparciu o umowę o pracę (załącznik do umowy o pracę)

Administratorem Pani/Pana danych osobowych jest Pan Tadeusz Seremet dyrektor Niepublicznej Szkoły Podstawowej im. „Akcji III Most" w Przybysławicach („Administrator"). Z Administratorem danych można się skontaktować telefonicznie pod numerem +48146283464 lub pisemnie na adres siedziby Administratora.
Pani/ Pana dane osobowe będą przetwarzane:
a) w celu realizacji obowiązków publicznoprawnych Administratora wynikających przede wszystkim z postanowień przepisów prawa w szczególności Kodeksu Pracy, przepisów ubezpieczeniowych, zdrowotnych, podatkowych, z zakresu bezpieczeństwa i higieny pracy – podstawą prawną jest wypełnienie obowiązków prawnych ciążących na Administratorze;
b) w celu realizacji zadań związanych z obsługą świadczeń pracowniczych – podstawą prawną jest wypełnienie obowiązków prawnych ciążących na Nowy Styl;
c) w celu organizacji wyjazdów służbowych i konferencji, w związku z realizacją zadań związanych z rozwojem ścieżki kariery zawodowej, zarządzania sprzętami udostępnianymi pracownikom w celu przygotowania stanowiska pracy – podstawą prawną przetwarzania danych jest prawnie uzasadniony interes polegający na zapewnieniu przez Administratora osobom zatrudnionym odpowiednich warunków i narzędzi pracy;
d) w celu realizacji wewnętrznych celów marketingowych oraz związanych z komunikacją wewnętrzną, będą przetwarzane dane w postaci wizerunku – podstawą prawną przetwarzania jest zgoda pracownika;
e) w celu ustalenia lub dochodzenia ewentualnych roszczeń lub obrony przed takimi roszczeniami przez Administratora – podstawą prawną przetwarzania danych jest prawnie uzasadniony interes Administratora polegający na umożliwieniu obrony praw przysługujących Administratorowi.

Pani/Pana dane osobowe będą przekazywane podmiotom świadczącym usługi na rzecz Administratora związane z wykonywaniem umowy o pracę, takim jak dostawcom systemów informatycznych i usług IT, operatorom pocztowym i kurierom, podmiotom prowadzącym szkolenia, bankom, podmiotom świadczącym usługi prawne, medyczne, ubezpieczycielom, kontrahentom i ich pracownikom w związku z realizacją obowiązków służbowych.
Pani/Pana dane osobowe będą przetwarzane przez okres trwania stosunku pracy. Okres przetwarzania danych osobowych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych osobowych będzie niezbędne dla dochodzenia ewentualnych roszczeń lub obrony przed takimi roszczeniami przez Administratora. Po tym okresie dane będą przetwarzane jedynie w zakresie i przez czas wymagany przepisami prawa. W przypadku gdy podstawą przetwarzania danych jest zgoda to dane będą przetwarzane do momentu jej wycofania.

Administrator informuje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także o prawie do przenoszenia danych oraz o prawie do wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych.

Niezależnie od powyższego w związku z tym, że podstawą przetwarzania danych osobowych jest przesłanka prawnie uzasadnionego interesu administratora, Administrator informuje, o prawie wniesienia sprzeciwu wobec przetwarzania danych osobowych.

Podanie danych jest wymagane na podstawie przepisów prawa. Brak podania danych będzie skutkował brakiem możliwości realizacji niektórych obowiązków lub uprawnień stron stosunku pracy. W zakresie w jakim przetwarzanie danych odbywa się w związku ze świadczeniami zapewnianymi przez Administratora na wniosek i w interesie pracownika, podanie danych jest wymagane w celu otrzymania takich świadczeń. Brak podania danych będzie skutkował niemożliwością otrzymania świadczenia. Podanie danych w celu realizacji wewnętrznych celów marketingowych oraz związanych z komunikacją wewnętrzną w postaci wizerunku, jest dobrowolne.

……

II. **Osoby zatrudnione w oparciu o umowę cywilnoprawną (załącznik do umowy)**

Administratorem Pani/Pana danych osobowych jest Pan Tadeusz Seremet dyrektor Niepublicznej Szkoły Podstawowej im. „Akcji III Most" w Przybysławicach („Administrator"). Z Administratorem danych można się skontaktować telefonicznie pod numerem +48146283464 lub pisemnie na adres siedziby Administratora.
Pani/ Pana dane osobowe będą przetwarzane:
a) w celu realizacji umowy – podstawą prawną jest realizacja umowy, której stroną jest podmiot danych;
b) w celu realizacji obowiązków publicznoprawnych Administratora wynikających przede wszystkim z przepisów podatkowych, przepisów dotyczących ochrony informacji niejawnych – podstawą prawną jest wypełnienie obowiązków prawnych ciążących na Administratorze;
c) w celu organizacji wyjazdów służbowych i konferencji, w związku z realizacją zadań związanych z rozwojem ścieżki kariery zawodowej, zarządzania sprzętami udostępnianymi współpracownikom – podstawą prawną przetwarzania danych jest prawnie uzasadniony interes Administratora polegający na zapewnieniu przez Administratora osobom współpracującym odpowiednich warunków i narzędzi pracy;
d) w celu ustalenia lub dochodzenia ewentualnych roszczeń lub obrony przed takimi roszczeniami przez Administratora – podstawą prawną przetwarzania danych jest prawnie uzasadniony interes Administratora polegający na umożliwieniu obrony praw przysługujących Administratorowi;
e) w celu realizacji wewnętrznych celów marketingowych oraz związanych z komunikacją wewnętrzną, będą przetwarzane dane w postaci wizerunku – podstawą prawną przetwarzania jest zgoda współpracownika.

Pani/Pana dane osobowe będą przekazywane podmiotom świadczącym usługi na rzecz Administratora związane z wykonywaniem zawartej umowy, takim jak dostawcom systemów informatycznych i usług IT, operatorom pocztowym i kurierom, podmiotom prowadzącym szkolenia, bankom, podmiotom świadczącym usługi prawne, medyczne, ubezpieczycielom.

Pani/Pana dane osobowe będą przetwarzane przez okres wykonywania umowy. Okres przetwarzania danych osobowych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych osobowych będzie niezbędne dla dochodzenia ewentualnych roszczeń lub obrony przed takimi roszczeniami przez Administratora. Po tym okresie dane będą przetwarzane jedynie w zakresie i przez czas wymagany przepisami prawa. W przypadku gdy podstawą przetwarzania danych jest zgoda to dane będą przetwarzane do momentu jej wycofania.

Administrator informuje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także o prawie do przenoszenia danych oraz o prawie do wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych.

Niezależnie od powyższego w związku z tym, że podstawą przetwarzania danych osobowych jest przesłanka prawnie uzasadnionego interesu administratora, Administrator informuje, o prawie wniesienia sprzeciwu wobec przetwarzania danych osobowych.

Podanie danych jest wymagane przez Administratora w celu wykonywania umowy, a brak ich podania będzie skutkował niemożliwością jej zawarcia i wykonania. W zakresie w jakim przetwarzanie danych odbywa się w związku ze świadczeniami zapewnianymi przez Administratora na wniosek i w interesie osoby współpracującej, podanie danych jest wymagane w celu otrzymania takich świadczeń. Brak podania danych będzie skutkował niemożliwością otrzymania świadczenia. Podanie danych w celu realizacji wewnętrznych celów marketingowych oraz związanych z komunikacją wewnętrzną w postaci wizerunku jest dobrowolne.

……

Klauzula informacyjna dla rodziców

1. Administratorem danych osobowych uczniów i rodziców jest Pan Tadeusz Seremet Dyrektor Niepublicznej Szkoły Podstawowej im. „Akcji III Most" w Przybysławicach, Przybysławice 152, 33-273 Marcinkowice. Z Administratorem można skontaktować się listownie na powyższy adres telefonicznie 146283464 lub e-mailowo przybyslawice.szkola@op.pl

2. Dane osobowe są przetwarzane na podstawie:
a) art. 6 ust. 1 lit. c RODO, tj. gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na placówce, w tym w związku z realizacją celów dydaktycznych, wychowawczych i opiekuńczych placówki w celu wykonania obowiązków prawnych nałożonych a ustawą z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz., 59) takich, jak prowadzenie ewidencji uczniów na potrzeby procesów nauczania, realizacja procesu nauczania, prowadzenie dziennika lekcyjnego, żywienie uczniów, prowadzenie zajęć dodatkowych, realizacja zadań z zakresu BHP, wypożyczanie książek z biblioteki szkolnej, prowadzenie świetlicy szkolnej;

b) art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez placówkę, w tym w związku ze stosowaniem monitoringu w celu zapewnienia bezpieczeństwa uczniów, pracowników i mienia placówki, prowadzeniem prac konserwatorskich i napraw infrastruktury informatycznej;

c) Art. 9 ust. 2 lit. h RODO w celu świadczenia opieki pielęgniarskiej i profilaktyki zdrowia uczniów, prowadzenia ewidencji uczniów na potrzeby procesów nauczania, realizacji procesu nauczania, realizacji zadań z zakresu BHP.

3. Prawnie uzasadnione interesy realizowane przez Administratora w związku z przetwarzaniem danych to zapewnienie bezpieczeństwa uczniów i pracowników, a także ochrony mienia placówki oraz zapewnienie prawidłowego funkcjonowania infrastruktury informatycznej w szkole.

4. Odbiorcami danych osobowych są upoważnieni pracownicy Administratora, podmioty, którym należy udostępnić dane osobowe w celu wykonania obowiązku prawnego, a także podmioty, którym dane zostaną powierzone do zrealizowania celów przetwarzania.

5. Dane osobowe będą przechowywane co najmniej do końca okresu, w którym uczeń będzie uczęszczał do placówki lub do czasu wycofania zgody, zgłoszenia sprzeciwu, a w każdym razie przez okres wskazany przepisami związanymi z wypełnianiem obowiązku prawnego przez placówkę.

6. Mają Państwo prawo żądania od Administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.

7. Mają Państwo prawo wnieść skargę do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych, jeśli uznają Państwo, iż przetwarzanie przez Administratora Państwa danych osobowych narusza przepisy dot. ochrony danych osobowych.

8. Podanie danych osobowych w celu wykonania przez Administratora obowiązku prawnego jest wymogiem ustawowym. W celu uczęszczania ucznia do placówki są Państwo zobowiązani do podania danych. Niepodanie danych skutkuje niemożnością realizowania zadań przez placówkę względem ucznia.

……

Klauzula informacyjna dotycząca monitoringu (rejestracja obrazu) na terenie Niepublicznej Szkoły Podstawowej im. „Akcji III Most" w Przybysławicach

Informujemy, że:

Administratorem Danych Osobowych (zwanym dalej ADO) systemu monitoringu wizyjnego (zwanym dalej Monitoring) jest Pan Tadeusz Seremet Dyrektor Niepublicznej Szkoły Podstawowej im. „Akcji III Most" w Przybysławicach, Przybysławice 152, 33-273 Marcinkowice.

Monitoring stosowany jest w celu rejestracji zdarzeń w celu zapewnienia bezpieczeństwa osobom przebywającym w budynku oraz najbliższym otoczeniu budynku, zapewnienia bezpieczeństwa infrastruktury i zasobów należących do ADO.

Obszar objęty monitoringiem stanowią korytarze siedziby Administratora oraz najbliższe otocznie na zewnątrz budynku Administratora.

Zarejestrowane dane nie podlegają profilowaniu, a przeglądanie danych odbywa się tylko w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa.

Zarejestrowane przez Monitoring dane osobowe będą przekazywane dostawcom systemów informatycznych i usług IT oraz podmiotom świadczącym na rzecz Administratora usługi w związku z prowadzeniem monitoringu (w tym podmiotom świadczącym usługi w zakresie ochrony osób i mienia).

Zapisy z monitoringu przechowywane będą przez okres do 30 dni. Po tym czasie zostaną nadpisane nowymi danymi.

Przysługuje Pani/Panu prawo: dostępu do treści danych oraz żądania ich sprostowania, usunięcia, ograniczenia przetwarzania.

Niezależnie od powyższego, w związku z tym, że podstawą przetwarzania danych osobowych jest przesłanka prawnie uzasadnionego interesu Administratora, Administrator informuje, o prawie wniesienia sprzeciwu wobec przetwarzania danych osobowych.

Przysługuje Pani/Panu także prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych , tj. Prezesa Urzędu Ochrony Danych Osobowych.

Podanie danych osobowych jest dobrowolne, ale niezbędne w celu umożliwienia wstępu na teren Obiektu Administratora, w tym w stosownych przypadkach, na obszar objęty monitoringiem. Konsekwencją niepodania danych będzie brak możliwości wstępu na teren Administratora.

……

Przybysławice, dnia ……..

Zgoda na wykorzystanie wizerunku dziecka

Zgodnie z art. 81 ust. 1 *Ustawy z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych (tj. Dz.U. 2017r. poz. 880 ze zm.)* wyrażam zgodę na nieodpłatne wykorzystywanie zdjęć oraz nagrań zawierających wizerunek mojego dziecka

……..... zarejestrowany podczas pobytu w Niepublicznej Szkole Podstawowej im. „Akcji III Most" w Przybysławicach w szczególności podczas uroczystości i zabaw organizowanych w placówce:

- konkursów,
- zajęć dydaktycznych,
- wycieczek, bez konieczności każdorazowego ich zatwierdzania.

Wykorzystanie wizerunku mojego dziecka ma na celu promowanie działalności placówki oraz osiągnięć i umiejętności dzieci. Zgoda dotyczy wizerunku zarejestrowanego w latach nauki mojego dziecka w Niepublicznej Szkole Podstawowej im. „Akcji III Most" w Przybysławicach.

Wyrażenie zgody jest jednoznaczne z tym, że wizerunek może zostać zamieszczony:

- strona internetowa placówki,
- Facebook,
- gabloty,
- kroniki,
- czasopisma (Radło, Gazeta Żabnieńska itp.)
- inne.

……
(Czytelny podpis rodzica/opiekuna)

Przybysławice, dnia ……..

Zgoda rodziców na udostępnienie danych wrażliwych dziecka

Wyrażam zgodę Administratorowi Panu Tadeuszowi Seremetowi dyrektorowi Niepublicznej Szkoły Podstawowej im. „Akcji III Most" w Przybysławicach na udostępnienie danych mojego dziecka w zakresie ……... …… (podać zakres), zgodnie z przepisami ustawy o ochronie danych osobowych i w celu……. ……...…… (podać cel).

Przyjmuję do wiadomości, że wymienione dane mają charakter wrażliwy i nie mogą być przetwarzane w innych celach i innym zakresie niż wskazuje niniejsza zgoda.

……

……
(Czytelne podpisy rodziców/opiekunów)

WZÓR
UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w …….. dnia …… r. pomiędzy:

Panem Tadeuszem Seremetem dyrektorem Niepublicznej Szkoły Podstawowej im. „Akcji III Most" w Przybysławicach, Przybysławice 152, 33-273 Marcinkowice
zwana dalej „**Administratorem**"
a
……,
zwana dalej „**Przetwarzającym**" lub „**Procesorem**"

1. DEFINICJE

Dla potrzeb niniejszej umowy, Administrator i Przetwarzający ustalają następujące znaczenie niżej wymienionych pojęć:

1) **Umowa Powierzenia** – niniejsza umowa;

2) **Umowa Główna** – [*umowa, w związku z którą zawierana jest umowa powierzenia – przetwarzanie danych jest konieczne do wykonania Umowy Głównej*]

3) **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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1).

2. OŚWIADCZENIA STRON

Strony oświadczają, że niniejsza Umowa Powierzenia została zawarta w celu wykonania obowiązków, o których mowa w art. 28 RODO w związku z zawarciem Umowy Głównej.

3. PRZEDMIOT UMOWY

3.1. W trybie art. 28 ust. 3 RODO, Administrator powierza Przetwarzającemu do przetwarzania dane osobowe wskazane w pkt 4.1.-4.2., a Przetwarzający zobowiązuje się do ich przetwarzania zgodnego z prawem i niniejszą Umową Powierzenia.

3.2. Przetwarzający może przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w Umowie Powierzenia, oraz zgodnie z innymi udokumentowanymi poleceniami Administratora, przy czym za takie udokumentowane polecenia uważa się postanowienia Umowy Powierzenia oraz ewentualne inne polecenia przekazywane przez Administratora drogą elektroniczną na adres ……. lub na piśmie.

4. CEL, ZAKRES I CHARAKTER PRZETWARZANIA

4.1. Przetwarzający zobowiązuje się do przetwarzania danych osobowych następujących kategorii osób, których dane dotyczą:

a) ……

b) ……

4.2. Zakres powierzonych Przetwarzającemu do przetwarzania danych osobowych obejmuje:

a) co do [*kategoria osób*]:

i. ……

b) co do [*kategoria osób*]:

i. ……

4.3. Celem i charakterem przetwarzania danych osobowych wskazanych w pkt 4.1.-4.2. powyżej jest wykonanie obowiązków/świadczenie usług wynikających z Umowy Głównej.

4.4. Dane osobowe będą przez Przetwarzającego przetwarzane w formie elektronicznej w systemach informatycznych oraz w formie papierowej.

4.5. Przetwarzający będzie otrzymywał dane osobowe od Administratora.

5. ZASADY POWIERZENIA PRZETWARZANIA

5.1. Przed rozpoczęciem przetwarzania danych osobowych Przetwarzający musi podjąć środki zabezpieczające dane osobowe, o których mowa w art. 32 RODO, a w szczególności:

a) uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Przetwarzający powinien odpowiednio udokumentować zastosowanie tych środków, a także uaktualniać te środki w porozumieniu z administratorem,

b) zapewnić, by każda osoba fizyczna działająca z upoważnienia Przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora w celach i zakresie przewidzianym w Umowie Powierzenia,

c) prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, o którym mowa w art. 30 ust. 2 RODO i udostępniać go Administratorowi na jego żądanie, chyba że Przetwarzający jest zwolniony z tego obowiązku na podstawie art. 30 ust. 5 RODO.

5.2. Przetwarzający zapewnia, aby osoby mające dostęp do przetwarzanych danych osobowych zachowały je oraz sposoby zabezpieczeń w tajemnicy, przy czym obowiązek zachowania tajemnicy istnieje również po realizacji Umowy Powierzenia oraz ustaniu zatrudnienia u Przetwarzającego.

6. DALSZE OBOWIĄZKI PRZETWARZAJĄCEGO

6.1. Przetwarzający zobowiązuje się pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO.

6.2. W sytuacji podejrzenia naruszenia ochrony danych osobowych, Przetwarzający zobowiązuje się do:

a) przekazania Administratorowi informacji dotyczących naruszenia ochrony danych osobowych w ciągu 12 godzin od jego wykrycia, w tym informacji, o których mowa w art. 33 ust. 3 RODO,

b) przeprowadzenia wstępnej analizy ryzyka naruszenia praw i wolności osób, których dane dotyczą, i przekazania wyników tej analizy do Administratora w ciągu 24 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych,

c) przekazania Administratorowi – na jego żądanie – wszystkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 34 ust. 3 RODO, w ciągu 24 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych.

6.3. Przetwarzający zobowiązuje się pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15-22 RODO. W szczególności Przetwarzający zobowiązuje się – na żądanie Administratora – do przygotowania i przekazania Administratorowi informacji potrzebnych do spełnienia żądania osoby, której dane dotyczą, w ciągu 3 dni od dnia otrzymania żądania Administratora.

6.4. Przetwarzający zobowiązuje się stosować się do ewentualnych wskazówek lub zaleceń, wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania RODO.

6.5. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych przez Przetwarzającego, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania powierzonych danych osobowych, skierowanej do Przetwarzającego, a także o wszelkich kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych przez Przetwarzającego, w szczególności prowadzonych przez organ nadzorczy.

6.6. Za nienależyte wykonywanie Umowy Powierzenia, w szczególności skutkujące dla Administratora zobowiązaniem prawomocną decyzją lub prawomocnym wyrokiem właściwego sądu do zapłaty kary pieniężnej, odszkodowania, zadośćuczynienia lub jakiejkolwiek innej kwoty z tytułu naruszenia przepisów dotyczących ochrony danych osobowych lub w związku ze szkodą lub krzywdą wyrządzoną w związku z naruszeniem przepisów dotyczących ochrony danych osobowych, Procesor odpowiada względem Administratora w pełnej wysokości i zobowiązany jest zwrócić

Administratorowi wszelkie koszty, wynikłe z tego dla Administratora, w tym w szczególności zwrócić kwotę wypłaconego odszkodowania, zadośćuczynienia lub kary pieniężnej, kosztów sądowych oraz kosztów zastępstwa procesowego.

7. PODPOWIERZENIE PRZETWARZANIA

7.1. Administrator dopuszcza możliwość podpowierzenia przetwarzania powierzonych danych osobowych podwykonawcom Przetwarzającego (tzw. subprocesorom). Jeżeli Przetwarzający zamierza podpowierzyć przetwarzanie danych osobowych swoim podwykonawcom, musi uprzednio poinformować Administratora o zamiarze podpowierzenia oraz o tożsamości (nazwie) podmiotu, któremu ma zamiar podpowierzyć przetwarzanie danych, a także o charakterze podpowierzenia, zakresie danych, celu i czasie trwania podpowierzenia. O ile Administrator nie wyrazi sprzeciwu wobec podpowierzenia w terminie 7 dni od daty zawiadomienia, Przetwarzający uprawniony będzie do dokonania podpowierzenia.

7.2. W przypadku podpowierzenia przetwarzania danych osobowych, podpowierzenie przetwarzania będzie mieć za podstawę umowę, na podstawie której podwykonawca (subprocesor) zobowiąże się do wykonywania tych samych obowiązków, które na mocy niniejszej Umowy Powierzenia nałożone są na Przetwarzającego. Umowa będzie zawarta w tej same formie co niniejsza Umowa Powierzenia.

7.3. Administratorowi będą przysługiwały uprawnienia wynikające z umowy podpowierzenia bezpośrednio wobec podwykonawcy (subprocesora). W przypadku wypowiedzenia lub rozwiązania umowy podpowierzenia, Przetwarzający poinformuje o tym fakcie Administratora w terminie 3 dni od wypowiedzenia lub rozwiązania umowy.

7.4. Przetwarzający nie może przekazywać powierzonych mu przetwarzania danych osobowych do podmiotów znajdujących się w państwach spoza Europejskiego Obszaru Gospodarczego.

8. AUDYT PRZETWARZAJĄCEGO

8.1. Administrator jest uprawniony do weryfikacji przestrzegania zasad przetwarzania danych osobowych wynikających RODO oraz niniejszej Umowy Powierzenia przez Przetwarzającego, poprzez prawo żądania udzielenia wszelkich informacji dotyczących powierzonych danych osobowych.

8.2. Administrator ma także prawo przeprowadzania audytów lub inspekcji Przetwarzającego w zakresie zgodności operacji przetwarzania z prawem i z Umową Powierzenia. Audyty lub inspekcje, o których mowa w zdaniu poprzedzającym, mogą być przeprowadzane przez podmioty trzecie upoważnione przez Administratora.

8.3. Przetwarzający zobowiązuje się niezwłocznie informować Administratora, jeżeli zdaniem Przetwarzającego wydane jemu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych.

9. ZAKOŃCZENIE POWIERZENIA PRZETWARZANIA

9.1. Umowa Powierzenia zostaje zawarta na czas określony i przestaje obowiązywać wraz z zakończeniem obowiązywania Umowy Głównej.

9.2. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych Przetwarzający zależnie od decyzji Administratora niezwłocznie usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie.

10. POSTANOWIENIA KOŃCOWE

10.1 Niniejsza Umowa podlega prawu polskiemu. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej Strony.

10.2 Zmiany Umowy Powierzenia wymagają zachowania formy pisemnej po rygorem nieważności.

10.3 Strona nie może przenieść praw lub obowiązków wynikających z Umowy bez uprzedniej zgody drugiej Strony wyrażonej w formie pisemnej pod rygorem bezskuteczności.

10.4 Wszelkie spory w związku z Umową zostaną poddane pod rozstrzygnięcie sądu powszechnego miejscowo właściwego zgodnie z Umową główną.

Administrator	**Procesor**
_____	_____

Klauzula obowiązku informacyjnego:

1. Administratorem Pani/Pana danych osobowych jest Pan Tadeusz Seremet dyrektor Niepublicznej Szkoły Podstawowej im. „Akcji III Most" w Przybysławicach, Przybysławice 152, 33-273 Marcinkowice („Administrator").
2. Z Administratorem można się skontaktować poprzez e-mail przybyslawice.szkola@op.pl lub pisemnie na adres siedziby Administratora.
3. Pani/Pana dane osobowe będą przetwarzane w celu obsługi żądania lub udzielenia odpowiedzi na pytanie przesłane za pośrednictwem formularza kontaktowego – podstawą prawną przetwarzania będzie prawnie uzasadniony interes Administratora; prawnie uzasadnionym interesem Administratora jest umożliwienie obsługi żądań oraz udzielania odpowiedzi na pytania zadawane przez osoby zainteresowane zasadami rekrutacji do w/w szkoły
4. Pani/Pana dane osobowe mogą być przekazywane dostawcom systemów informatycznych i usług IT, działającym na zlecenie Administratora.
5. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do obsługi żądania lub udzielenia odpowiedzi przez Administratora.
6. Przysługuje Pani/Panu prawo: dostępu do treści danych oraz żądania ich sprostowania, usunięcia i ograniczenia przetwarzania.
7. Niezależnie od powyższego, w związku z tym, że podstawą przetwarzania danych osobowych jest przesłanka prawnie uzasadnionego interesu administratora, Administrator informuje o prawie wniesienia sprzeciwu wobec przetwarzania danych osobowych.
8. Przysługuje Pani/Panu także prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.
9. Podanie danych jest konieczne do obsługi żądania lub udzielenia odpowiedzi ma pytanie przez Administratora. Konsekwencją niepodania danych osobowych będzie brak możliwości obsługi żądania lub udzielenia odpowiedzi na przesłane przez Panią/Pana pytanie.