Zespół Szkół Centrum Kształcenia
Rolniczego im. Władysława Grabskiego
w Sędziejowicach
Sędziejowice-Kolonia 10, 98-160 Sędziejowice
tel./fax 43 67 710 04
Regon 000095615 NIP 831-14-40-538

Zarządzenie Dyrektora Nr 52/2022

Zespołu Szkół Centrum Kształcenia Rolniczego

im. Władysława Grabskiego w Sędziejowicach

z dnia 01 września 2022 r.

w sprawie

wprowadzenia Polityki bezpieczeństwa i ochrony przetwarzania danych osobowych wraz z instrukcją zarządzania systemem informatycznym, oraz procedurą zarządzania naruszeniami w Zespole Szkół Centrum Kształcenia Rolniczego im. Władysława Grabskiego w Sędziejowicach

Na podstawie § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (jt. Dz.U. z 2017 r., poz. 2247), art. 24 ust.1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

zarządzam, co następuje:

§ 1.

Wprowadzam do stosowania:

Politykę bezpieczeństwa i ochrony przetwarzania danych osobowych wraz z instrukcją zarządzania systemem informatycznym, oraz procedurą zarządzania naruszeniami w Zespole Szkół Centrum Kształcenia Rolniczego im. Władysława Grabskiego w Sędziejowicach

§ 2.

Wszyscy pracownicy placówki zobowiązani są do zapoznania się z Polityką i stosowania uregulowań w niej zawartych. Instrukcja stanowi załącznik do zarządzenia.

§ 3.

Polityka bezpieczeństwa i ochrony przetwarzania danych osobowych wraz z instrukcją zarządzania systemem informatycznym, oraz procedurą zarządzania naruszeniami w Zespole Szkół Centrum Kształcenia Rolniczego im. Władysława Grabskiego w Sędziejowicach jest przeznaczona do użytku wewnętrznego i nie podlega publikacji.

§ 4.

Traci moc zarządzenie Nr 12/2020 z dnia 31 sierpnia 2020 roku.

§ 5.

Zarządzenie wchodzi w życie z dniem 01 września 2022 r.

DYREKTOR
Zespołu Szkół Centrum Kształcenia
Rolniczego im. Władysława Grabskiego
w Sędziejowicach
mgr Beata Magdziak

Załącznik do Zarządzenia nr ..52../2022

Dyrektora Zespołu Szkół Centrum Kształcenia Rolniczego w Sędziejowicach

Z dnia 01.09.2022 roku

ZESPÓŁ SZKÓŁ CENTRUM KSZTAŁCENIA ROLNICZEGO im. Władysława Grabskiego W SĘDZIEJOWICACH

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

W ZESPOLE SZKÓŁ CENTRUM KSZTAŁCENIA ROLNICZEGO

IM. WŁADYSŁAWA GRABSKIEGO

W SĘDZIEJOWICACH

Sędziejowice, dnia 1 września 2022

SPIS TREŚCI

1. WPROWADZENIE

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich ochrony w Zespole Szkół Centrum Kształcenia Rolniczego im. Władysława Grabskiego w Sędziejowicach, zwanym dalej **SZKOŁĄ.**

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym wyrażone w Polityce bezpieczeństwa oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Wszelkie zestawienia uzupełniające treść dokumentu zebrano w postaci załączników. Do najważniejszych należy ewidencja zbiorów osobowych, miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych, a także lista środków organizacyjnych i technicznych służących bezpieczeństwu danych.

2. PODSTAWY PRAWNE

2.1. USTAWA ORAZ AKTY WYKONAWCZE

Przepisy ochrony danych osobowych zawarte są w ustawie o ochronie danych osobowych oraz wydanych do niej aktach wykonawczych. Pełną listę aktów prawnych stanowią:

- 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)
- USTAWA z dnia 10 maja 2018 r. o ochronie danych osobowych

Niniejszy dokument powstał w oparciu o art. od 5 do 39 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r, które zobowiązują Administratora danych do wykonania dokumentacji opisującej środki organizacyjne i techniczne służące ochronie przetwarzanych danych osobowych.

2.2. DEFINICJE

W dokumencie przyjmuje się następującą terminologię:

Urząd Ochrony Danych Osobowych (UODO) – organ do spraw ochrony danych osobowych.

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Dane wrażliwe - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Administrator Danych Osobowych (ADO) – organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. ADO w szkole jest **Dyrektor**.

Inspektor Ochrony Danych Osobowych (IODO) – osoba nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

Rejestr czynności przetwarzania danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

3. NAJWAŻNIEJSZE ZAGADNIENIA OCHRONY DANYCH OSOBOWYCH

3.1. PREZES URZĄD OCHRONY DANYCH OSOBOWYCH

Zadania Prezesa UODO

Do zadań Prezesa UODO należy:

- kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

- wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych,
- prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach,
- opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,
- inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
- uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.
- stworzenie mechanizmu certyfikacji organizacji
- nakładanie kar finansowych za nieprzestrzeganie przepisów o ochronie danych osobowych
- prowadzenie systemu, który umożliwi zgłaszanie administratorom naruszeń danych osobowych w wyznaczonym przez RODO czasie

Kontrole UODO

W celu wykonania w/w zadań Prezes UODO, zastępca prezesa UODO lub upoważnieni przez niego pracownicy Urzędu, zwani dalej „inspektorami", mają prawo:

- wstępu, w godzinach od 6°° do 22°°, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
- żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
- wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,
- przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,
- zlecać sporządzanie ekspertyz i opinii.

Działania Prezesa UODO w przypadku naruszenie przepisów

W przypadku naruszenia przepisów o ochronie danych osobowych Prezes UODO z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:

- usunięcie uchybień,
- uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,
- zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,
- wstrzymanie przekazywania danych osobowych do państwa trzeciego,
- zabezpieczenie danych lub przekazanie ich innym podmiotom,
- usunięcie danych osobowych
- nałożyć karę grzywny

W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Prezes UODO kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

3.2. PRZETWARZANIE DANYCH

Przetwarzanie danych jest **dopuszczalne** tylko wtedy gdy:

- Osoba, której dane dotyczą, **wyrazi na to zgodę**, chyba że chodzi o usunięcie dotyczących jej danych. Zgoda może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. Zgoda nie może być domniemana lub dorozumiana. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie zgody nie jest możliwie, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.
- Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia **obowiązku wynikającego z przepisu prawa**.
- Jest to konieczne do **realizacji umowy**, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.
- Jest niezbędne do **wykonania określonych prawem zadań** realizowanych dla dobra publicznego.
- Jest to niezbędne dla **wypełnienia prawnie usprawiedliwionych celów** realizowanych przez Administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Przetwarzanie danych jest **zabronione** w przypadku danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzanie tych danych **jest jednak dopuszczalne**, jeżeli:

- osoba, której dane dotyczą, **wyrazi na to zgodę na piśmie**, chyba że chodzi o usunięcie dotyczących jej danych,
- **przepis szczególny innej ustawy zezwala** na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,
- przetwarzanie takich danych jest **niezbędne do ochrony żywotnych interesów osoby**, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,
- jest to niezbędne do wykonania **statutowych zadań kościołów i innych związków wyznaniowych**, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,
- przetwarzanie dotyczy danych, które są niezbędne **do dochodzenia praw przed sądem**,
- przetwarzanie jest **niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób**, a zakres przetwarzanych danych jest określony w ustawie,
- przetwarzanie jest prowadzone **w celu ochrony stanu zdrowia**, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,
- przetwarzanie dotyczy danych, które zostały podane **do wiadomości publicznej przez osobę**, której dane dotyczą,
- jest to niezbędne do **prowadzenia badań naukowych**, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,
- przetwarzanie danych jest prowadzone przez stronę **w celu realizacji praw i obowiązków wynikających z orzeczenia** wydanego w postępowaniu sądowym lub administracyjnym.

3.3. OBOWIĄZKI INFORMACYJNE O PRZETWARZANIU DANYCH

Zbieranie danych osobowych od osób, których dane dotyczą

W przypadku zbierania danych od osoby, której te dane dotyczą Administrator danych jest zobowiązany poinformować tę osobę o:

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy Administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- Wskazaniu danych kontaktowych Inspektora Ochrony Danych Osobowych
- celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- ewentualnym zamiarem przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej
- prawie dostępu do treści swoich danych oraz ich poprawiania,

- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Zbieranie danych osobowych nie od osób, których dane dotyczą.

W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator danych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu danych o:

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
- źródle danych,
- prawie dostępu do treści swoich danych oraz ich poprawiania,
- prawie wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,
- prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy Administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Podanych wyżej zasad **nie stosuje się**, jeżeli:

- dane są przetwarzane przez administratora na podstawie przepisów prawa,
- przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
- dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania.

3.4. UDOSTĘPNIANIE DANYCH

Najważniejsze przesłanki i zasady udostępniania danych:

- Nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie.
- Nie ma znaczenia (ujmując problem technicznie) czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd.
- Udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa.
- Dane osobowe, z wyłączeniem danych wrażliwych, mogą być udostępniane nie w oparciu o przepisy prawa, jeżeli osoba wnioskująca w sposób wiarygodny uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
- Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
- Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

3.5. POWIERZENIE PRZETWARZANIA DANYCH

W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla Administratora danych może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami:

- umowa powinna być zawarta niezależnie od posiadanej umowy określającej relacje obu stron,
- Podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianym w umowie,
- Podmiot, któremu powierzono przetwarzanie danych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy oraz spełnić wymagania określone w przepisach, o których mowa w art.39a ustawy. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych,
- odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na Administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

3.6. DOKUMENTOWANIE

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Ponadto, Administrator danych:

- prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki organizacyjne i techniczne służące ochronie danych,
- wyznacza Inspektora Ochrony Danych Osobowych, nadzorującego przestrzeganie zasad ochrony chyba, że sam wykonuje te czynności,
- nadaje upoważnienia do przetwarzania danych i dopuszcza do pracy wyłącznie osoby posiadające takie upoważnienie,
- zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
- prowadzi ewidencję osób upoważnionych do ich przetwarzania, która zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a także identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Minister właściwy do spraw administracji publicznej w porozumieniu z ministrem właściwym do spraw informatyzacji określi, w drodze **rozporządzenia**, sposób prowadzenia i zakres dokumentacji opisującej ochronę danych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną,

a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.

3.7. SANKCJE KARNE

W razie stwierdzenia naruszeń RODO organ nadzorczy jest uprawniony w szczególności do:

- wydawania ostrzeżeń przedsiębiorcom przetwarzającym dane osobowe dotyczących możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania;
- udzielania upomnień przedsiębiorcom przetwarzającym dane osobowe w przypadku naruszenia przepisów RODO przez operacje przetwarzania;
- nakazania przedsiębiorcom przetwarzającym dane osobowe spełnienia żądań osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO;
- nakazania przedsiębiorcom przetwarzającym dane osobowe dostosowania operacji przetwarzania do przepisów RODO, a w szczególności, w stosownych przypadkach wskazania sposobu i terminu dostosowania;
- nakazania przedsiębiorcom przetwarzającym dane osobowe zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- wprowadzenia czasowego lub całkowitego ograniczenia przetwarzania danych, w tym zakazu przetwarzania;
- nakazania sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazania powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;
- cofnięcia certyfikacji lub nakazania podmiotowi certyfikującemu cofnięcia certyfikacji lub nakazania podmiotowi certyfikującemu nieudzielenia certyfikacji;
- nakazania zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

Niezależnie od ww. środków naprawczych, organ nadzorczy jest uprawniony do nakładania na przedsiębiorcę, który naruszył postanowienia RODO, kary pieniężnej. Ww. środki naprawcze będą mogły być nakładane na przedsiębiorców zamiast lub obok innych sankcji, w tym obok administracyjnych kar pieniężnych.

4. ZAGROŻENIA BEZPIECZEŃSTWA

4.1. PROCEDURA ZARZĄDZANIA NARUSZENIAMI

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

- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3) Jeżeli informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

4) Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

5) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu

6) Zawiadomienie, o którym mowa w pkt 5, nie jest wymagane, w następujących przypadkach:
a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4.2. CHARAKTERYSTYKA MOŻLIWYCH ZAGROŻEŃ

- **Zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona lecz nie dochodzi do naruszenia poufności danych.
- **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych,
- **zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

4.3. SYTUACJE ŚWIADCZĄCE O NARUSZENIU ZASAD BEZPIECZEŃSTWA

- **Przełamane zabezpieczenia tradycyjnych** – zerwane plomby na drzwiach, szafach, segregatorach,
- **sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych** na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
- **niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
- **awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
- **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- **jakość danych w systemie** lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- **naruszenie lub próba naruszenia integralności** systemu lub bazy danych w tym systemie,
- **próba lub modyfikacja danych** oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- **niedopuszczalna manipulacja** danymi osobowymi w systemie,
- **ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu,
- **praca w systemie lub jego sieci komputerowej wykazująca nieprzypadkowe odstępstwa** od założonego rytmu pracy oraz wskazująca na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
- **ujawnienie istnienia nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki", itp.,
- **podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowania lub kopiowanie danych,
- **rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji** (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

4.4. TABELE FORM NARUSZENIA BEZPIECZEŃSTWA I SPOSOBY POSTĘPOWANIA

Tabela form naruszenia ochrony danych osobowych przez osoby zatrudnione przy przetwarzaniu danych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona,
Ujawnianie informacji o sprzęcie i pozostałej	

infrastrukturze informatycznej.	powiadomić Inspektora Ochrony Danych Osobowych.
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport
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 do takiej sytuacji. Sporządzić raport.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić Inspektora Ochrony Danych Osobowych. Sporządzić raport.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić Inspektora Ochrony Danych Osobowych. Sporządzić raport.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Sporządzić raport.
Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.
W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić Inspektora Ochrony Danych Osobowych. Sporządzić raport.

Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić Inspektora Ochrony Danych Osobowych. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru nie zamkniętego 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 pomieszczenie. Powiadomić przełożonych. Sporządzić raport.
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i Inspektora Ochrony Danych Osobowych. Sporządzić raport.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Inspektora Ochrony Danych Osobowych. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Inspektora Ochrony Danych Osobowych. Sporządzić raport.
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Inspektora Ochrony Danych Osobowych. Sporządzić raport.

Tabela zjawisk świadczących o możliwości naruszenia ochrony danych osobowych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie Inspektora Ochrony Danych Osobowych oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	
Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	

Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	
Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie Inspektora Ochrony Danych Osobowych. Sporządzić raport.

Tabela naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić Inspektora Ochrony Danych Osobowych. Sporządzić raport.
Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	

5. POLITYKA BEZPIECZEŃSTWA

Polityka bezpieczeństwa rozumiana jest jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Instytucji. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

5.1. DEKLARACJA

Administrator danych mając świadomość, iż przetwarza dane **wrażliwe** uczniów deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.

W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumenty te są uzupełniane załącznikami do dokumentacji, na które składają się m.in.: wykazy zbiorów, miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych.

W celu zapewnienia prawidłowego monitorowania przetwarzania danych wprowadza się liczne ewidencje, które szczegółowo charakteryzują obszary objęte monitoringiem, umożliwiając pełną kontrolę nad tym, jakie dane i przez kogo są przetwarzane oraz komu udostępniane.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

5.2. CHARAKTERYSTYKA INSTYTUCJI

Szkoła realizuje zadania głównie na mocy przepisów prawa zawartych w ustawie Prawo Oświatowe, Kodeks Pracy, systemie informacji oświatowej oraz Karcie Nauczyciela, a także innych aktach wykonawczych uprawniających Dyrektora szkoły do podejmowania stosownych działań, w tym do przetwarzania danych osobowych. Podstawowym obszarem działania są zadania związane z bezpłatnym nauczaniem.

5.3. WYKAZ ZBIORÓW OSOBOWYCH

Na podstawie art. od 5 do 39 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r **tworzy się wykaz zbiorów osobowych wraz ze wskazaniem programów komputerowych oraz rejestr czynności przetwarzania danych oraz rejestr kategorii czynności** służących do ich przetwarzania zgodnie z **załącznikiem nr 1** do niniejszej dokumentacji.

Z uwagi na połączenie komputerów z siecią Internet, dla zbiorów przetwarzanych elektronicznie stosuje się, zgodnie z § 6 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. środki bezpieczeństwa na poziomie **WYSOKIM**.

5.4. WYKAZ MIEJSC PRZETWARZANIA

Na podstawie art. od 5 do 39 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r tworzy się wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych.

Wyznaczają go pomieszczenia zlokalizowane w Szkole. Szczegółowy wykaz pomieszczeń, stanowi **załącznik nr 2** do niniejszej dokumentacji.

5.5. EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. od 5 do 39 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi **załącznik nr 3** do niniejszej dokumentacji.

Ewidencja zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania uprawnień oraz zakres, a w przypadku kiedy dane są przetwarzane za pomocą programu komputerowego również identyfikator dostępowy do tego programu.

Ewidencja stanowi podstawę wydania Upoważnienia do przetwarzania danych.

5.6. ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

- Przetwarzanie danych osobowych w Szkole może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- Zgodnie z art. 37 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r, Administrator danych **powołuje Inspektora Ochrony Danych Osobowych (IODO).**

- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne **upoważnienie**. Wzór upoważnienia stanowi **załącznik nr 4** do niniejszej dokumentacji.
- IODO prowadzi **ewidencję osób upoważnionych** oraz na jej podstawie przygotowuje **Upoważnienia do przetwarzania danych** i przedkłada je do podpisu ADO.
- Unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego **załącznik nr 5** do niniejszej dokumentacji.
- Zabrania się przetwarzania danych poza obszarem określonym w załączniku nr 2 do niniejszej instrukcji.
- Każdy pracownik Szkoły co najmniej raz na 2 lata musi odbyć **szkolenie z zakresu ochrony danych** osobowych. Za organizację szkoleń odpowiedzialny jest IODO, który prowadzi w tym celu odpowiednią dokumentację. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.
- Ponadto każdy upoważniony do przetwarzania danych **potwierdza pisemnie** fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi **załącznik nr 6** do niniejszej dokumentacji. Podpisany dokument jest dołączany do akt osobowych.
- Obszar przetwarzania danych osobowych określony w załączniku nr 2 do niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Dostęp do obszaru monitorują służby bezpośredniej ochrony.
- Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych. Wzory zgody na przebywanie w pomieszczeniach dla osób nie posiadających upoważnienia, a także odwołania tej zgody, stanowią odpowiednio **załącznik nr 7** oraz **załącznik nr 8** do przedmiotowej dokumentacji.
- Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
- Przetwarzanie danych podawanych dobrowolnie może odbywać się tylko na podstawie pisemnej zgody podającego te dane wg wzoru określonego w **załączniku nr 10.**

Dla zapewnienia kontroli przestrzegania zasad określonych w niniejszej dokumentacji wyznacza się następujące **zadania Inspektorowi Ochrony Danych Osobowych:**

- Realizację powierzonych obowiązków zawartych w dokumencie „Zakres Obowiązków, uprawnień i odpowiedzialności IODO oraz:
- Nadzór nad przetwarzaniem danych zgodnie z Rozporządzeniem Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r i innymi przepisami prawa.
- Kontrola przestrzegania zasad ochrony – systematycznie, nie rzadziej niż dwa razy do roku kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom

nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w szczególności:

- Kontrola dokumentacji opisującej sposób przetwarzania oraz ochrony.
- Kontrola fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są informacje.
- Kontrola poprawności zabezpieczeń danych przetwarzanych metodami tradycyjnymi.
- Kontrola awaryjnego zasilania komputerów.
- Nadzór nad naprawą, konserwacją oraz likwidacją urządzeń komputerowych.
- Kontrola systemu kontroli obecności wirusów komputerowych.
- Kontrola wykonywania kopii awaryjnych.
- Kontrola przeglądu, konserwacji oraz uaktualnienia systemów informatycznych.
- Kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych.
- Kontrola nadanych upoważnień.

- Przedstawianie Administratorowi danych wyników kontroli.
- Systematyczna analiza dokumentacji pod kątem obszarów, zbiorów oraz zasad ochrony.
- Szkolenie z ochrony danych osobowych oraz aktów wykonawczych.
- Podjęcie natychmiastowych działań zabezpieczających w przypadku otrzymania informacji o naruszeniu bezpieczeństwa informacji.
- Prowadzenie monitoringu przetwarzania danych.
- Każdorazowe sporządzenie raportu zgodnie ze wzorem będącym **załącznikiem nr 9** do niniejszej dokumentacji oraz przedstawienie efektów działań Administratorowi danych.

5.7. ŚRODKI TECHNICZNE OCHRONY DANYCH OSOBOWYCH

Zbiory danych przetwarzane w Szkole zabezpiecza się poprzez:

1. **Środki ochrony fizycznej.**

- Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
- Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
- Zbiory danych osobowych przechowywane są w pomieszczeniach, w których okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
- Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
- Dostęp do budynków pomieszczeń, w których przetwarzane są zbiory danych osobowych przez cała dobę jest dozorowany.
- Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej metalowej szafie.

- Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętym sejfie lub kasie pancernej.
- Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętym zamkniętej metalowej szafie lub kasie pancernej.
- Pomieszczenia, w którym przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
- Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

2. **Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej.**
   - Zbiory danych osobowych przetwarzane są przy użyciu komputera stacjonarnego.
   - Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
   - Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
   - Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
   - Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
   - Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
   - Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
   - Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
   - Użyto system Firewall do ochrony dostępu do sieci komputerowej.

3. **Środki ochrony w ramach systemowych narzędzi programowych i baz danych.**
   - Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych.
   - Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanych zbiorów danych osobowych.
   - Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
   - Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
   - Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych.
   - Zastosowano kryptograficzne środki ochrony danych osobowych.
   - Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

- Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określa **Instrukcja zarządzania systemem informatycznym** służącym do przetwarzania danych osobowych opisana w pkt 6 niniejszej dokumentacji.

6. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

I. CHARAKTERYSTYKA SYSTEMU

1. Sieć informatyczna ma strukturę zwielokrotnionej gwiazdy ze switchem centralnym, do którego podłączone są punkty dostępowe AP (WiFi) oraz komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.
2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.
3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku oraz na wybranych stanowiskach zasilaczami awaryjnymi utrzymującymi stałe zasilanie.

II. OGÓLNE ZASADY PRACY W SYSTEMIE INFORMATYCZNYM

1. IODO odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.
2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez IODO do eksploatacji licencjonowane oprogramowanie.
3. IODO prowadzi ewidencję oprogramowania.
4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
   a. mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu,
   b. mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej,
   c. mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
   d. urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,
   e. mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,
   f. mechanizmy zarządzania zmianami.
5. Użytkownikom zabrania się:
   a. korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy Szkoły bez pisemnej zgody ADO,
   b. udostępniania stanowisk roboczych osobom nieuprawnionym,
   c. wykorzystywania sieci komputerowej Szkoły w celach innych niż wyznaczone przez ADO,

d. samowolnego instalowania i używania programów komputerowych,

e. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,

f. umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej Szkoły, oraz sieci Internetowej osobom nieuprawnionym,

g. używania komputera bez zainstalowanego oprogramowania antywirusowego.

III. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI.

1. Użytkowników systemu informatycznego tworzy oraz usuwa IODO na podstawie zgody ADO.
2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
3. Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi załącznik nr 3 do niniejszej dokumentacji.
4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:
    a. nieobecności pracownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
    b. zawieszenia w pełnieniu obowiązków służbowych.
5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

IV. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.

1.

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator, którego nazwa składa się z trzech pierwszych liter imienia oraz trzech pierwszych nazwiska.
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika IODO, nadaje inny identyfikator odstępując od ogólnej zasady.
4. W identyfikatorze pomija się polskie znaki diakrytyczne.
5. Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny.
6. Zmianę hasła należy dokonywać nie rzadziej niż co 30 dni.

7. Hasła użytkowników generuje IODO i przekazuje wraz z loginem w formie papierowej w zamkniętej kopercie.
8. Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do ich zniszczenia w odpowiednim urządzeniu niszczącym.
9. Hasło nie może być zapisywane i przechowywane.
10. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

V. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY.

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.
3. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.
4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3.
5. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.
6. IODO monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

VI. PROCEDURY TWORZENIA KOPII AWARYJNYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA.

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.
2. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
3. Zabezpieczeniu poprzez wykonywanie kopii awaryjnych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
4. Za proces tworzenia kopii awaryjnych na serwerze (jeśli jest) odpowiada IODO.
5. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, użytkownicy systemu informatycznego zobowiązani są do wykonywania samodzielnie kopii bezpieczeństwa tych zbiorów.
6. Kopie awaryjne mogą być wykonywane tylko na nośnikach informatycznych dostarczonych przez IODO.
7. Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
8. Kopie awaryjne wykonuje się ostatniego dnia każdego miesiąca lub częściej, w zależności od potrzeb.
9. Kopie awaryjne przechowuje IODO, a w przypadku przetwarzania danych na stacjach roboczych poszczególni użytkownicy. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności.

10. IODO zobowiązany jest do okresowego wykonywania testów odtworzeniowych kopii awaryjnych.
11. Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, zaś po upływie czasu ich przydatności – niszczone w niszczarkach dokumentów.

VII. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI.

1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu informatycznego, przechowuje IODO w odpowiednio zabezpieczonym pomieszczeniu.
2. Dane osobowe gromadzone są wyłącznie serwerze jeśli takowy jest elementem systemu informatycznego. Zabrania się gromadzenia danych osobowych na innych nośnikach danych.
3. W uzasadnionych przypadkach, za zgodą IODO, dane osobowe można przetwarzać na dyskach twardych komputerów stacjonarnych lub zarejestrowanych nośnikach informacji dostarczonych przez IODO.
4. Przenośne nośniki danych powinny być zabezpieczone ochroną kryptograficzną.
5. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
    a. **likwidacji** — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
    b. **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
    c. **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ABI.
6. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym przez IODO.

VIII. SPOSÓB ZABEZPIECZENIA SYSTEMU PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO.

1. IODO zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody. System antywirusowy jest skonfigurowany w następujący sposób:
    a. skanowanie dysków zawierających potencjalnie niebezpieczne dane następuje automatycznie po włączeniu komputera,
    b. skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.
    c. Automatycznej aktualizacji wzorców wirusów.
2. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie IODO.
3. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, IODO podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

a. usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,

b. odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,

c. samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.

4. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.

5. IODO monitoruje stan systemu, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system.

IX. INFORMACJE O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPNIONE, DACIE I ZAKRESIE TEGO UDOSTĘPNIENIA.

1. Informacje o udostępnieniu danych osobowych przetwarza się i przechowuje w oparciu o Rzeczowy Wykaz Akt i Instrukcję kancelaryjną.

2. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest ADO.

3. Nadzór nad właściwym udostępnianiem danych prowadzi IODO.

X. PRZESYŁANIE DANYCH POZA OBSZAR PRZETWARZANIA

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.

2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:

   a. zatwierdzenie przez IODO zakresu danych osobowych przeznaczonych do wysłania,
   b. zastosowanie mechanizmów szyfrowania danych osobowych,
   c. zastosowanie mechanizmów podpisu elektronicznego zabezpieczającego transmisje danych osobowych oraz rejestrację transmisji wysyłania danych osobowych.

3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

4. IODO tworzy konfigurację mechanizmów kryptograficznych w sposób:

   a. zapewniający wykorzystanie obowiązujących wymagań w zakresie kryptograficznej ochrony danych osobowych,

   b. umożliwiający, w miarę technicznych możliwości, automatyczne szyfrowanie danych osobowych wysyłanych poza obszar przetwarzania danych,

   c. informujący użytkownika o dołączeniu do wysyłanych danych osobowych elektronicznego podpisu i wymagający przed wysłaniem informacji potwierdzenia podpisywanej treści.

5. IODO jest odpowiedzialny za realizację procesów związanych z zarządzaniem aplikacjami kryptograficznymi oraz generowanie kluczy dostępowych do tych aplikacji.

XI. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH.

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO.
2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez IODO.
3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez IODO.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza Szkołą, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.
5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.
6. IODO wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

7. ZAŁĄCZNIKI

Załącznik nr 1. Wykaz zbiorów osobowych przetwarzanych w Szkole.

Załącznik nr 2. Wykaz miejsc przetwarzania zbiorów osobowych w Szkole.

Załącznik nr 3. Wykaz osób upoważnionych do przetwarzania danych osobowych w Szkole.

Załącznik nr 4. Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 5. Wzór unieważnienia upoważnienia do przetwarzania danych osobowych.

Załącznik nr 6. Wzór potwierdzenia znajomości zasad bezpieczeństwa.

Załącznik nr 7. Wzór zgody na przebywanie w obszarze przetwarzania danych osobowych.

Załącznik nr 8. Wzór odwołania zgody na przebywanie w obszarze przetwarzania danych osobowych.

Załącznik nr 9. Wzór raportu z naruszenia bezpieczeństwa zasad ochrony danych osobowych.

Załącznik nr 10. Wzór zgody na przetwarzanie danych dla pracownika oraz dla rodziców uczniów.

Załącznik nr 11. Rejestr czynności przetwarzania danych oraz rejestr kategorii czynności

DYREKTOR
Zespołu Szkół Centrum Kształcenia
Rolniczego im. Władysława Grabskiego
w Sędziejowicach
mgr Beata Magdziak

WYKAZ ZBIORÓW OSOBOWYCH

Lp.	Nazwa zbioru - opis	Podstawa prawna przetwarzania	Struktura zbioru	Program
1.	Księga Uczniów - Zbiór danych o uczniach	§ 3. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 24 sierpnia 2011 r. w sprawie sposobu prowadzenia przez publiczne szkoły i placówki artystyczne dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2011 r. Nr 187, poz. 1118), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, przyjęcie do szkoły: data, klasa , obwód szkolny, profil kierunek zawód specjalność Wypisanie ze szkoły: data, klasa, powody, Data: wydania dok, ukończenia szkoły numer wydanego świadectwa (dyplomu)	
2.	Dziennik lekcyjny - Dokumentacja przebiegu nauczania w danym roku szkolnym	§ 4.3. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 24 sierpnia 2011 r. w sprawie sposobu prowadzenia przez publiczne szkoły i placówki artystyczne dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2011 r. Nr 187, poz. 1118), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu,	Dziennik Lekcyjny firmy Vulcan.
3.	Arkusz Ocen - dokumentacja wyników nauczania ucznia w poszczególnych latach	§ 6. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 24 sierpnia 2011 r. w sprawie sposobu prowadzenia przez publiczne szkoły i placówki artystyczne dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2011 r. Nr 187, poz. 1118), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, nr księgi uczniów, przebieg nauki, wyniki nauki	Dziennik Lekcyjny firmy Vulcan
4.	Ewidencja świadectw szkolnych	§ 5.3. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 15 marca 2012 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych szkół i placówek artystycznych (Dz. U. z 2012 r. poz. 377 z późn. zm.).	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel	
5.	Ewidencja legitymacji szkolnych	§ 5. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 15 marca 2012 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych szkół i placówek artystycznych (Dz. U. z 2012 r. poz. 377 z późn. zm.).	Nazwiska, imiona, pesel	
6.	Dokumentacja dotycząca kandydatów przystępujących do egzaminu wstępnego do szkoły (osoby nie rozpoczęły nauki).	§ 5 i 6 rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 15 maja 2014 r. w sprawie warunków i trybu przyjmowania uczniów do publicznych szkół i publicznych placówek artystycznych oraz przechodzenia z jednych typów szkół do innych (Dz. U. z 2014 r., poz. 686), art. 20n ust. 10 ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256, poz. 2572, z późn. zmianami	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zameldowania, zamieszkania, pesel, , telefon, nazwa szkoły	UONET+ firmy Vulcan
7.	Księga arkuszy ocen - zbiór arkuszy ocen uczniów urodzonych w jednym roku, którzy ukończyli lub opuścili szkołę	§ 7.2.3. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 24 sierpnia 2011 r. w sprawie sposobu prowadzenia przez publiczne szkoły i placówki artystyczne dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2011 r. Nr 187, poz. 1118), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Nr księgi uczniów, przebieg nauki, wyniki nauki	
8.	Ewidencje decyzji administracyjnych dyrektora.	Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z dnia 24 sierpnia 2011 r. w sprawie sposobu prowadzenia przez publiczne szkoły i placówki artystyczne dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2011 r. Nr 187, poz. 1118), art. 22 ust. 2 pkt 5 ustawy z dnia 7	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania	Pakiet biurowy Office

		września 1991 r. o systemie oświaty.		
9.	Protokoły Rady Pedagogicznej - Protokoły z posiedzenia Rady Pedagogicznej	§ 1.2. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 24 sierpnia 2011 r. w sprawie sposobu prowadzenia przez publiczne szkoły i placówki artystyczne dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2011 r. Nr 187, poz. 1118), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, data urodzenia, stan zdrowia	
10.	Okręgowa Komisja Egzaminacyjna	§ 52.1. oraz § 74.7. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 8 kwietnia 2008 r. w sprawie warunków i sposobu oceniania, klasyfikowania i promowania uczniów oraz przeprowadzania sprawdzianów i egzaminów w publicznych szkołach i placówkach artystycznych (Dz. U. z 2008 r. Nr 65, poz. 400 z późn. zm.).	Nazwisko, imiona, data i miejsce urodzenia, Pesel, płeć, dysleksja, mniejszość narod.	**Hermes**
11.	Stypendia	art. 90f, 90g ustawy z dnia 7 września 1991 r. o systemie oświaty	Imię, nazwisko, data urodzenia, adres zamieszkania, PESEL, NIP, imiona i nazwiska rodziców, adresy zamieszkania, dochody	
12.	Zwolnienia lekarskie uczniów z wychowania fizycznego – decyzje dyrektora szkoły	§ 6.2. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 8 kwietnia 2008 r. w sprawie warunków i sposobu oceniania, klasyfikowania i promowania uczniów oraz przeprowadzania sprawdzianów i egzaminów w publicznych szkołach i placówkach artystycznych (Dz. U. z 2008 r. Nr 65, poz. 400 z późn. zm.).	Imię i nazwisko	
13.	Wyprawka szkolna	rozporządzenie Rady Ministrów z 29 lipca 2014 r. w sprawie szczegółowych warunków udzielania pomocy finansowej uczniom na zakup podręczników i materiałów edukacyjnych (Dz.U. poz. 1024).	Nazwisko, imię ucznia, data urodzenia, miejsce urodzenia, adres zamieszkania, imiona i nazwiska rodziców, adres zamieszkania, dochód	Pakiet biurowy Office
14.	Biblioteka	art. 67.1 pkt 2) ustawy z dnia 7 września 1991 r. o systemie oświaty	Nazwisko, imię, adres zam., dane o wypożyczeniach	MOL Vulcan
15.	Dziennik Pedagoga - Dziennik zawiera informacje o dzieciach zakwalifikowanych do różnych form pomocy	§ 5.3. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 24 sierpnia 2011 r. w sprawie sposobu prowadzenia przez publiczne szkoły i placówki artystyczne dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2011 r. Nr 187, poz. 1118), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, Informacje o kontaktach z innymi osobami, instytucjami, stan zdrowia	Dziennik Lekcyjny firmy Vulcan
16.	Dokumentacja Pedagoga - Dokumentacja badań i czynności uzupełniających prowadzonych przez pedagoga	§ 5.6. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 24 sierpnia 2011 r. w sprawie sposobu prowadzenia przez publiczne szkoły i placówki artystyczne dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2011 r. Nr 187, poz. 1118), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Różne dane niezbędne do dokumentowania przebiegu terapii, nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, stan zdrowia, opinia PPP	Pakiet biurowy Office
17.	Karty zdrowia ucznia		Nazwisko i imię, wiek, data urodzenia, adres zamieszkania, PESEL, informacje o stanie zdrowia	
18.	Lista uczestników wycieczek	§ 7.3 pkt 5 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 8 listopada 2001 r. w sprawie warunków i sposobu organizowania przez publiczne przedszkola, szkoły i placówki krajoznawstwa i turystyki.	Nazwisko i imię, wiek, data urodzenia, adres zamieszkania, PESEL	Pakiet biurowy Office
19.	Ubezpieczenie uczniów	Zgoda osób	Imiona nazwiska, adres zamieszkania lub pobytu	

20.	Dokumentacja wypadków uczniów - Informacje o wypadkach uczniów	§ 43.3 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach.	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, stan zdrowia	
21.	Księga ewidencji wychowanków internatu	§ 75 rozporządzenia Ministra Edukacji Narodowej z dnia 21 lutego 1994 r. w sprawie rodzajów, organizacji zasad działania publicznych placówek opiekuńczo- wychowawczych i resocjalizacyjnych. (Dziennik Ustaw Rzeczpospolitej Polskiej Nr 41 z 28 marca 1994r. z późn. zm.)	Imię (imiona) i nazwisko, datę i miejsce urodzenia oraz adres zamieszkania dziecka, a także imiona i nazwiska rodziców (prawnych opiekunów) oraz adresy ich zamieszkania	
22.	Dzienniki zajęć wychowawczych w internacie	§ 76 rozporządzenia Ministra Edukacji Narodowej z dnia 21 lutego 1994 r. w sprawie rodzajów, organizacji zasad działania publicznych placówek opiekuńczo- wychowawczych i resocjalizacyjnych. (Dziennik Ustaw Rzeczpospolitej Polskiej Nr 41 z 28 marca 1994r. z późn. zm.)	Imię (imiona) i nazwisko, datę i miejsce urodzenia oraz adres zamieszkania dziecka, a także imiona i nazwiska rodziców (prawnych opiekunów) oraz adresy ich zamieszkania	Dziennik Lekcyjny firmy Vulcan
23.	Opinie i Orzeczenia Poradni Psychologiczno-Pedagogicznej	§ 4 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 7 stycznia 2003 r. w sprawie zasad udzielania i organizacji pomocy psychologiczno-pedagogicznej w publicznych przedszkolach, szkołach i placówkach (Dz. U. z dnia 29 stycznia 2003 r.)	Imię i nazwisko, data urodzenia, stan zdrowia	
24.	Wnioski rodziców o naukę religii i etyki	§ 1.1 pkt 1 rozporządzenia Ministra Edukacji Narodowej z dnia 14 kwietnia 1992 r. w sprawie warunków i sposobu organizowania nauki religii w publicznych przedszkolach i szkołach (tekst jednolity Dz. U. 1993 nr 83 poz. 390)	Imię, nazwisko, dziecka oraz imiona i nazwiska rodziców i adresy zamieszkania, przynależność wyznaniowa	
25.	Dziennik zajęć pozalekcyjnych	§ 5.5. rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 24 sierpnia 2011 r. w sprawie sposobu prowadzenia przez publiczne szkoły i placówki artystyczne dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2011 r. Nr 187, poz. 1118), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Imię i nazwisko, adres zamieszkania	Dziennik Lekcyjny firmy Vulcan
26.	Zgody na przetwarzanie danych	Zgoda osób	Imię i nazwisko adres udzielającego zgodę	Pakiet biurowy Office
27.	Ewidencja wejść i wyjść do internatu	Zgoda osób	Nazwisko, imię, nr dowodu toż.	
28.	Akta osobowe - Zbiór zatrudnionych pracowników	Art. 22 oraz 229 § 7 ustawy z dnia 26.06.1974 Kodeks pracy	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, wykształcenie, przebieg dotychczasowego zatrudnienia, daty urodzenia dzieci, imiona i nazwiska dzieci, stan zdrowia	Kadry, Płace
29.	Rejestr zaświadczeń wydanych pracownikom,		Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL,	Program Płatnik
30.	Listy płac pracowników		Nazwiska i imiona, poszczególne składniki wynagrodzenia	Płatnik, Płace, Kadry, ePFRON,
31.	Deklaracje podatkowe		Nazwiska i imiona, imiona rodziców, data	ePITY

	pracowników,		urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL	
32.	System Informacji Oświatowej Zbiór zawiera informacje o nauczycielach i uczniach szkoły	Art. 3.4 Ustawy z dnia 19 lutego 2004 r. o systemie informacji oświatowej, Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 16 grudnia 2004 r. w sprawie szczegółowego zakresu danych w bazach danych oświatowych, zakresu danych identyfikujących podmioty prowadzące bazy danych oświatowych, terminów przekazywania danych między bazami danych oświatowych oraz wzorów wydruków zestawień zbiorczych	PESEL, miejsce pracy, zawód, wykształcenie, wynagrodzenie	SIO
33.	Komisja Socjalna - Świadczenia dla pracowników	Art. 8 ust. 2 ustawy z dnia 4.03.1994 o zakładowym funduszu świadczeń socjalnych	Nazwiska i imiona, adres zamieszkania lub pobytu, stan zdrowia	
34.	Dobrowolne ubezpieczenie pracowników	Zgoda osób	Imiona nazwiska, adres zamieszkania lub pobytu, PESEL, nr telefonu	
35.	Dokumentacja wypadków pracowników - Informacje o wypadkach pracowników	§ 1.2 rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 19 grudnia 2002 r. (Dz. U. Nr 236, poz. 1992) § 4.1 Rozporządzenia Ministra Gospodarki i Pracy z 16.9.2004 r. w sprawie wzoru protokołu ustalenia okoliczności i przyczyn wypadku przy pracy - Dz. U. Nr 227, poz. 2298	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, stan zdrowia	
36.	Umowy zlecenia	Art. 734 – 751 ustawy z dnia 23 kwietnia 1964 r. Kodeks Cywilny (Dz. U. z dnia 18 maja 1964 r.)	Nazwiska i imiona, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, nr telefonu	Pakiet biurowy Office
37.	Przelewy	Ustawa o rachunkowości	Nazwiska, imiona, adresy zamieszkania, nr kont bankowych kontrahentów będących osobami fizycznymi, NIP, wyciągi bankowe	Programy Homenet, Foka, Magazyn Optivum
38.	Klienci	art. 23.1 pkt 3 ustawy o ochronie danych osobowych	Nazwisko, imię, adres, PESEL, NIP, dowód osobisty	
39.	Faktury	art. 23.1 pkt 3 ustawy o ochronie danych osobowych	Nazwisko, imię, adres zamieszkania	
40.	Książka korespondencyjna	Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 1999 r. w sprawie instrukcji kancelaryjnej dla organów gmin i związków międzygminnych (Dz.U. z 1999 r. Nr 112, poz. 1319 z późn.zm.).	Imię i nazwisko, adres zamieszkania	
41.	Ubezpieczenie ZUS - Informacje o pracownikach potrzebne do ubezpieczenia w ZUS	Art. 36.10 oraz art.41.3 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, PESEL, NIP	Płatnik
42.	Kasa zapomogowo-pożyczkowa	art. 39 ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. Nr 55 poz. 234), Rozporządzenie Rady Ministrów z dnia 19 grudnia 1992 r. w sprawie pracowniczych kas zapomogowo-pożyczkowych w zakładach pracy (Dz. U. Nr 100 poz. 502 z późn. zm.) oraz § 7.1 Rozporządzenia Rady	Nazwisko, Imię, Imiona rodziców, Data urodzenia, Miejsce zamieszkania, imię i nazwisko oraz adres zamieszkania osoby uposażonej do odebrania świadczeń na wypadek śmierci, dane osobowe poręczycieli, wysokości pożyczki.	

		Ministrów z dnia 19 grudnia 1992 w sprawie pracowniczych kas zapomogowo pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy (Dz. U 100 poz. 502)		

43.	Awans Zawodowy	Art. 9 a, 9 b ust 1 pkt 2ustawy z dnia 26 stycznia 1982 rok Karta Nauczyciela (Dz. U. z 2006 Nr 97 poz. 674 z późn. zm.)	Imiona, nazwisko, nazwisko rodowe, data urodzenia, adres zam. przebieg zatrudnienia, wykształcenie.	Windows, Pakiet biurowy Office
44.	Monitoring wizyjny	Art. 6 ust. 1 lit f) RODO - prawnie uzasadniony interes administratora, tj. w celu zachowania w tajemnicy informacji, których ujawnienie mogłyby narazić Administratora na szkodę, co umożliwia przepis art. 22 § 1 ustawy z dnia z dnia 26 czerwca 1974 r. – Kodeks pracy, art. 45 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742) oraz § 4 ust. 3 pkt 6 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U. z 2012 r. poz. 683 ze zm.)	Wizerunki osób	Rejestrator obrazu z monitoringu

WYKAZ MIEJSC PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa pomieszczenia	Adres
	Sekretariat	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Gabinet dyrektora	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Gabinet wicedyrektora.	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Pracownia fizyczna	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Księgowość.	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Kadry	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Pokój nauczycielski.	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Pedagog szkolny.	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Internat – pokój wychowawców	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Internat. Intendentka.	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Biblioteka.	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*
	Kierownik szkolenia praktycznego	*Sędziejowice-Kolonia 10, 98-160 Sędziejowice*

WYKAZ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwisko, Imię	Nr zbiorów	Okres upoważnienia		Program/	Uwagi
			OD	DO	identyfikator	
1	Augustajtys Dorota	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	20.06.2018		Dziennik elektroniczny, Pakiety biurowe Office,	Nauczyciel
2	Bendkowski Piotr	1,2,3,4,5,6,7,8,9,10,11,1 2,13,18,19,20,23,24,25,2 6,28,29,32,34,35,36,37,3 8,39,40,42,43	20.06.2018		Microsoft Office, SIO/administrator, pakiety biurowe Office	IODO, administrator SSI, nauczyciel
3	Bobrowski Szymon	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2020		Dziennik elektroniczny, Pakiety biurowe Office	nauczyciel
4	Dymińska Marlena	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	20.06.2018		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel
5	Hachulska-Jędraszek Lidia	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	20.06.2018		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel
6	Kasprzycka Katarzyna	1-44	01.09.2022		Pakiety biurowe Office,	Wicedyrektor, nauczyciel
7	Sowa Jerzy	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2022		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel
8	Miszczak Paulina	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2022		Dziennik elektroniczny, Pakiety biurowe Office	nauczyciel
9	Kopytowska Marta	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	20.06.2018		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel
10	Marciniak-Kulka Ewa	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2022		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel
11	Krystyniak Magalena	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2020		Dziennik elektroniczny, Pakiety biurowe Office	nauczyciel
12	Krysztofiak Marek	1,2,3,9,18,25	20.06.2018		Pakiety biurowe Office,	Samodzielny referent
13	Machała Anna	1,3,9,4,5,6,7,8,10,11,12, 13,17,18,19,20,21,24,26, 32,34,38,39,40,42	20.06.2018		Pakiety biurowe Office, SIO,	Sekretarka
14		37,38,39	20.06.2018		Pakiety biurowe Office,	Starszy magazynier
15	Najdler Jakub	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2020		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel, wychowawca w internacie
16	Pasowska Magdalena	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2020		Dziennik elektroniczny, Pakiety biurowe Office	nauczyciel
17		1-43	20.06.2018		Pakiety biurowe Office, Księgowość, Faktury, Rejestr, Inwentarz (pakiet Vulcan Optivum), SJO Bestia, Druki Infor, Epuap	Księgowa
18	Kowalczyk Anna	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2022		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel
19	Kaczmarek Łukasz	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2022		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel
20	Sowjak Tomasz	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	20.06.2018		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel

21	**Szymański Tomasz**	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2020		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel
22	**Trzuskowski Jarosław**	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2020		Dziennik elektroniczny, Pakiety biurowe Office	nauczyciel
23	**Witczak Elżbieta**	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2020		Dziennik elektroniczny, Pakiety biurowe Office	nauczyciel
24	**Wojtczak Ewa**	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	01.09.2020		Dziennik elektroniczny, Pakiety biurowe Office	nauczyciel
25	**Zięterska Wioletta**	1-44	20.06.2018		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel, kierownik szkolenia
26	**Zimny Agnieszka**	1,2,3,4,9,11,12,13,18,19, 23,24,25,26	20.06.2018		Dziennik elektroniczny, Pakiety biurowe Office	Nauczyciel

Stan na dzień 31 sierpnia 2022

.....

(Piotr Bendkowski –IODO)

Sędziejowice, dnia .....r.

ZSR – ...../2020/IODO

(sygnatura)

WAŻNOŚĆ:
od: 01.09.2020
do: do odwołania

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO (GDPR),** ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z dn. 24 maja 2018, poz. 1000) oraz ustawy o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. (Dz. U. Nr 144, poz. 1204 ze zm.) niniejszym upoważniam Panią/Pana:

Nazwisko i Imię: .....

Stanowisko: .....

do przetwarzania, w ramach wykonywanych obowiązków służbowych, następujących zbiorów danych osobowych:

Nr zbiorów z ewidencji zbiorów *	Nazwa programu / identyfikator

Jednocześnie, wraz z nadanym upoważnieniem, zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Inspektora Ochrony Danych Osobowych dokumentu POLITYKA BEZPIECZEŃSTWA I OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH WRAZ Z INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM ORAZ PROCEDURĄ ZARZĄDZANIA NARUSZENIAMI oraz Instrukcji Zarządzania. Niniejsze upoważnienie traci moc najpóźniej z dniem odwołania albo rozwiązania lub wygaśnięcia umowy o prace, umowy zlecenia, umowy o dzieło lub innej umowy cywilnoprawnej łączącej Pana/Panią z Administratorem.

Upoważnienie obejmuje uprawnienie do przetwarzania danych w zakresie niezbędnym do realizacji powierzonych zadań wynikających z warunków zatrudnienia.

.....
(podpis osoby upoważnianej)

.....
(podpis Administratora Danych Osobowych)

*) Wykaz zbiorów zawarty jest w dokumencie POLITYKA BEZPIECZEŃSTWA I OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH WRAZ Z INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM dostępnym w sekretariacie, u Administratora Danych Osobowych i u Inspektora Ochrony Danych Osobowych

Sędziejowice, dnia .....r.

.....

(sygnatura)

UNIEWAŻNIENIE

Na podstawie Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r oraz Ustawy z dnia 10 maja 2018 o Ochronie Danych Osobowych unieważniam upoważnienie do przetwarzania danych osobowych wydane

dnia ..... o sygnaturze ..... dla Pani/Pana:

.....

.....

(podpis Administratora Danych Osobowych)

Sędziejowice, dnia .....r.

.....

(imię i nazwisko pracownika)

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść:
   a) Polityki bezpieczeństwa i ochrony przetwarzania danych osobowych wraz z instrukcją zarządzania systemem informatycznym w Zespole Szkół Rolniczych im. Władysława Grabskiego w Sędziejowicach,
   b) Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (tekst jednolity: Dz. U. 2018 r. poz. 1000),
   c) Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016

2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy, a w szczególności nie będę:
   a) ujawniać danych zawartych w eksploatowanych w systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
   b) ujawniać szczegółów technologicznych używanych w systemów oraz oprogramowania,
   c) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
   d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą Polityką bezpieczeństwa i ochrony przetwarzania danych osobowych wraz z instrukcją zarządzania systemem informatycznym w Zespole Szkół Centrum Kształcenia Rolniczego im. Władysława Grabskiego w Sędziejowicach.

.....

(podpis pracownika)

.....

(podpis Administratora Danych Osobowych)

Sędziejowice, dnia .....r.

ZSR – ...../2020/IODO

(sygnatura)

WAŻNOŚĆ:
od: 01.09.2020
do: do odwołania

ZGODA

NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO (GDPR),** ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z dn. 24 maja 2018, poz. 1000) niniejszym **wyrażam zgodę Pani/Panu:**

Nazwisko i Imię: .....

Stanowisko: .....

na przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania obowiązków służbowych.

Jednocześnie, wraz z nadanym upoważnieniem, zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Inspektora Ochrony Danych Osobowych dokumentu POLITYKA BEZPIECZEŃSTWA I OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH WRAZ Z INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM ORAZ PROCEDURĄ ZARZĄDZANIA NARUSZENIAMI oraz Instrukcji Zarządzania. Niniejsze upoważnienie traci moc najpóźniej z dniem odwołania albo rozwiązania lub wygaśnięcia umowy o prace, umowy zlecenia, umowy o dzieło lub innej umowy cywilnoprawnej łączącej Pana/Panią z Administratorem.

Upoważnienie obejmuje uprawnienie do przebywanie w miejscach przetwarzania danych osobowych w zakresie niezbędnym do realizacji powierzonych zadań wynikających z warunków zatrudnienia bez możliwości przetwarzania danych osobowych.

.....
(podpis osoby upoważnianej)

.....
(podpis Administratora Danych Osobowych)

*) Wykaz zbiorów zawarty jest w dokumencie POLITYKA BEZPIECZEŃSTWA I OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH WRAZ Z INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM dostępnym w sekretariacie, u Administratora Danych Osobowych i u Inspektora Ochrony Danych Osobowych

Sędziejowice, dnia .....r.

.....

(sygnatura)

ODWOŁANIE ZGODY

NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r oraz Ustawy z dnia 10 maja 2018 o Ochronie Danych Osobowych **odwołuję zgodę** z dnia ..... o sygnaturze ..... udzieloną **Pani/Panu:**

.....

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe.

.....

(podpis Administratora Danych Osobowych)

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych

w .....

1. Data: .... Godzina: .....
(dd.mm.rr) *(gg:mm)*

Inspektor Ochrony Danych Osobowych: Piotr Bendkowski, tel: 602 49 48 54

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące (kategorie i przybliżona liczba osób, których dane dotyczą, oraz kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie):
.....
.....
.....
.....
.....
.....

5. Przyczyny wystąpienia zdarzenia:
.....
.....
.....

6. Środki zastosowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków:
.....
.....
.....

7. Możliwe konsekwencje naruszenia ochrony danych osobowych:
.....
.....
.....

.....
(data, podpis Inspektora Ochrony Danych Osobowych)

Sędziejowice, dnia .....r.

.....

.....

.....

(imię i nazwisko, adres zamieszkania)

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH PRACOWNIKA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z 27 kwietnia 2016 r. informujemy, iż:

1. Administratorem Pani/Pana danych osobowych jest Zespół Szkół Centrum Kształcenia Rolniczego im. Władysława Grabskiego, Sędziejowice-Kolonia 10, 98-160 Sędziejowice
2. Inspektorem Ochrony Danych w Zespole Szkół Centrum Kształcenia Rolniczego w Sędziejowicach jest Pan Piotr Bendkowski e-mai: administrator@zsrgrabski.pl
3. Pani/Pana dane osobowe przetwarzane będą w celu zawarcia lub przedłużenia umowy o pracę lub innej umowy cywilno-prawnej, wypłaty wynagrodzenia oraz innych czynności związanych z powierzonymi zadaniami służbowymi wynikającymi z Kodeksu Pracy lub Ustawy Prawo Oświatowe.
4. Zakresem monitoringu wizyjnego objęty jest obszar wokół siedziby Administratora, ciągi komunikacyjne budynku oraz kluczowe pomieszczenia. Administrator przechowuje nagrania przez trzy (3) miesiące od dnia nagrania. W związku z tym Pani/Pana dane osobowe będą przetwarzane w celu zapewnienia bezpieczeństwa pracowników oraz współpracowników Administratora, ochrony jego mienia oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Administratora na szkodę, co stanowi prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f) RODO).
5. Pani/Pana dane osobowe są przetwarzane zgodnie z ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z dn. 24 maja 2018, poz. 1000) oraz ustawą o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. (Dz. U. Nr 144, poz. 1204 ze zm.).
6. Nasze działania są zgodne z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
7. Odbiorcą Pani/Pana danych osobowych będzie Zespół Szkół Centrum Kształcenia Rolniczego im. Władysława Grabskiego w Sędziejowicach
8. Pani/Pana dane osobowe będą przechowywane przez okres 50 lat
9. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania *(jeżeli przetwarzanie odbywa się na podstawie zgody)*, którego dokonano na podstawie zgody przed jej cofnięciem;
10. Ma Pan/Pani prawo wniesienia skargi do UODO gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r (RODO).
11. Podanie przez Pani/Pana danych osobowych jest niezbędne do zawarcia/przedłużenia umowy. W przypadku niepodania danych niemożliwe jest zawarcie/przedłużenie umowy.
12. Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

.....

(podpis)

Sędziejowice, dnia .....r.

.....

.....

.....

(imię i nazwisko, adres zamieszkania)

ZGODA RODZICA NA PRZETWARZANIE DANYCH OSOBOWYCH DZIECKA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z 27 kwietnia 2016 r. informujemy, iż:

1. Administratorem Pani/Pana danych osobowych oraz danych osobowych Pani/Pana córki/syna jest Zespół Szkół Centrum Kształcenia Rolniczego im. Władysława Grabskiego, 98-160 Sędziejowice
2. Inspektorem ochrony danych w Zespole Szkół Centrum Kształcenia Rolniczego w Sędziejowicach jest Pan Piotr Bendkowski e-mail: administrator@zsrgrabski.pl
3. Pani/Pana dane osobowe oraz dane osobowe Pani/Pana córki/syna przetwarzane będą w celu podejmowania działań edukacyjnych szkoły, prowadzenia konkursów, promocji osiągnięć i utrwalania pozytywnego wizerunku szkoły, w szczególności poprzez zamieszczanie informacji na jej stronie internetowej, oraz realizacji innych działań oświatowych, kulturalnych, sportowych czy edukacyjnych, promowanie działań związanych z realizacją celów dydaktycznych, wychowawczych i opiekuńczych poprzez upowszechnianie zdjęć oraz materiałów filmowych.
4. Zakresem monitoringu wizyjnego objęty jest obszar wokół siedziby Administratora, ciągi komunikacyjne budynku oraz kluczowe pomieszczenia. Administrator przechowuje nagrania przez trzy (3) miesiące od dnia nagrania. W związku z tym dane osobowe Pani/Pana córki/syna będą przetwarzane w celu zapewnienia bezpieczeństwa pracowników oraz współpracowników Administratora, ochrony jego mienia oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Administratora na szkodę, co stanowi prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f) RODO).
5. Pani/Pana dane osobowe oraz dane osobowe Pani/Pana córki/syna są przetwarzane zgodnie z ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z dn. 24 maja 2018, poz. 1000) oraz ustawą o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. (Dz. U. Nr 144, poz. 1204 ze zm.).
6. Nasze działania są zgodne z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
7. Odbiorcą Pani/Pana danych osobowych oraz danych osobowych Pani/Pana córki/syna będzie Zespół Szkół Centrum Kształcenia Rolniczego im. Władysława Grabskiego w Sędziejowicach
8. Pani/Pana dane osobowe oraz dane osobowe Pani/Pana córki/syna będą przechowywane przez okres 10 lat
9. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania *(jeżeli przetwarzanie odbywa się na podstawie zgody)*, którego dokonano na podstawie zgody przed jej cofnięciem;
10. Ma Pan/Pani prawo wniesienia skargi do UODO gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r (RODO).;
11. Podanie przez Pani/Pana danych osobowych oraz danych osobowych Pani/Pana córki/syna jest wymogiem ustawowym. Jest Pan/Pani zobowiązana do ich podania a konsekwencją niepodania danych osobowych będzie nie przyjęcie Pani/Pana dziecka do szkoły.

.....

(czytelny podpis osoby akceptującej klauzulę)