Polityka Ochrony
Danych Osobowych
w Szkole Podstawowej nr 2
im. bł. Edmunda Bojanowskiego
w Woli Rzędzińskiej

ZATWIERDZAM

.....
(data i podpis Administratora Danych)

I. POSTANOWIENIA OGÓLNE ... 2
DEKLARACJA I ZASTOSOWANIE ... 2
DEFINICJE ... 3
ZASADY OCHRONY DANYCH ... 4
ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH ... 5
II. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH ... 6
III. PRZEDSIĘWZIĘCIA ZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH ... 8
IV. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH ... 9
DZIAŁANIA KORYGUJĄCE I ZAPOBIEGAWCZE ... 9
ZGŁASZANIE NARUSZEŃ ... 9
V. DOSTĘP DO DANYCH OSOBOWYCH ... 9
VI. PRAWA PODMIOTÓW DANYCH ... 10
POROZUMIENIA I KONTAKTY ZE STRONAMI ZEWNĘTRZNYMI ... 10
VII. GRUPY INFORMACJI PODLEGAJĄCE OCHRONIE I REJESTR CZYNNOŚCI ... 11
VIII. BEZPIECZEŃSTWO OSOBOWE ... 12
ETAP NABORU PRACOWNIKA I WSPÓŁPRACOWNIKA ... 12
EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH ... 12
ZATRUDNIENIE / WSPÓŁPRACA ... 13
ZAKOŃCZENIE ZATRUDNIENIA / WSPÓŁPRACY ... 13
ZASADY PRZYZNAWANIA DOSTĘPU ... 14
IX. BEZPIECZENSTWO TELEINFORMATYCZNE ... 14
AUTORYZACJA I DOPUSZCZALNE WYKORZYSTANIE ZASOBÓW ... 14
METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM ... 16
X. POSTANOWIENIA KOŃCOWE ... 17
XI. SPIS ZAŁĄCZNIKÓW ... 18

I. POSTANOWIENIA OGÓLNE

§ 1

DEKLARACJA I ZASTOSOWANIE

1. **Celem** niniejszej Polityki Ochrony Danych Osobowych (PODO) jest wypełnienie założeń 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, dalej też zwane RODO).
2. Stanowi ona zbiór wymogów, zasad i regulacji ochrony danych osobowych u **Administratora danych osobowych**, którym jest: **Szkoła Podstawowa nr 2 w Woli Rzędzińskiej** reprezentowany przez: ***dyrektora szkoły*** , (dalej jako ADO).
3. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce Ochrony Danych Osobowych (PODO lub Polityka), obowiązują wszystkich pracowników i współpracowników ADO.
4. Procedury i dokumenty związane z Polityką będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku. Wzór *Planu audytów i przeglądów Polityki Ochrony Danych Osobowych* stanowi **załącznik nr 7** do niniejszej Polityki.
5. Polityka określa środki techniczne i organizacyjne zastosowane przez ADO dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym lub w kartotekach papierowych, albo w sytuacji podejrzenia o takim naruszeniu.
6. Polityka została opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania właściwej ochrony wraz z zachowaniem ich integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.
7. Zakres obowiązywania dokumentu.
   1) Niniejsza Polityka obowiązuje wszystkich pracowników, współpracowników, a także kontrahentów ADO.
   2) Każdy z pracowników i współpracowników ma obowiązek zapoznania się z treścią niniejszej Polityki.
   3) Polityka dotyczy wyposażenia, systemów, urządzeń przetwarzających informacje w formie elektronicznej, papierowej lub jakiejkolwiek innej.
   4) Nieprzestrzeganie postanowień zawartych w Polityce może skutkować sankcjami w pełnym zakresie dopuszczonym przez stosunek pracy oraz obowiązujące przepisy prawa.
   5) W celu skutecznego zapoznania pracowników i współpracowników z zasadami zawartymi w niniejszej Polityce wprowadza się zestaw reguł stanowiący wyciąg najistotniejszych zapisów zawartych w Polityce i w *Instrukcji zarządzania systemem informatycznym* stanowiącej **załącznik nr 12** do niniejszej Polityki.

Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest ADO, a za nadzór i monitorowanie jej przestrzegania odpowiada: ***Inspektor ochrony danych (dalej IOD).***

§ 2

DEFINICJE

- **administrator danych - „**administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych**; Administratorem jest: Szkoła Podstawowa nr 2 w Woli Rzędzińskiej** *reprezentowany przez dyrektora* (dalej jako **ADO**).
- **administrator Systemu Informatycznego (ASI) –** rozumie się przez to osobę odpowiedzialną za nadzór nad systemami informatycznymi wykorzystywanymi u Administratora Danych. Wyznaczenie i obowiązki ASI opisuje **załącznik nr 2** do niniejszej Polityki.
- **bezpieczeństwo informacji –** zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność**;**
- **dane osobowe -** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- **dane szczególne** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
- **eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;
- **hasło** – rozumie się przez to ciąg znaków alfanumerycznych, znany jedynie użytkownikowi;
- **identyfikator** – rozumie się przez to, ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- **incydent ochrony danych osobowych –** zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia ochrony danych osobowych;
- **Inspektor Ochrony Danych (IOD) –** osoba sprawująca nadzór nad przestrzeganiem zasad ochrony danych osobowych wyznaczona przez ADO; *wyznaczenie i zakres obowiązków IOD* opisuje **załącznik nr 1**, a *regulamin IOD* **załącznik nr 14** do niniejszej Polityki.
- **naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- **obszar przetwarzania danych** – rozumie się przez to budynki i pomieszczenia określone przez administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione; obszar przetwarzania danych opisany jest w **załączniku nr 3** do niniejszej Polityki;
- **odbiorca danych –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być

zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania**;**

- **osoba, podmiot danych -** oznacza osobę, której dane dotyczą;
- **podmiot przetwarzający -** oznacza organizację lub osobę, której ADO powierzył przetwarzanie danych osobowych (np. usługodawca IT, dostawca ESOK czy innego systemu informatycznego);
- **polityka** oznacza niniejszą politykę ochrony danych osobowych;
- **postępowanie z ryzykiem –** proces planowania i wdrażania działań wpływających na ryzyko;
- **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
- **profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
- **raport** – rozumie się przez to przygotowanie przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
- **RCPDO lub rejestr** oznacza rejestr czynności przetwarzania danych osobowych;
- **RODO** oznacza rozporządzenie parlamentu europejskiego i rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we (ogólne rozporządzenie o ochronie danych) (dz.urz. UE l 119, s. 1).
- **ryzyko –** niepewność osiągnięcia zamierzonych celów**;**
- **serwisant** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;
- **system informatyczny administratora danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;
- **szacowanie ryzyka –** proces identyfikowania, analizowania i oceniania ryzyka;
- **teczka ODO** – zbiór dokumentów, instrukcji, regulaminów, załączników opisujących sposób przetwarzania i ochrony danych, składający się na politykę ochrony danych osobowych, gromadzonych i nadzorowanych przez IOD.
- **teletransmisja** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
- **uwierzytelnienie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- **użytkownik** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;
- **zgoda** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 3

ZASADY OCHRONY DANYCH

System zarządzania ochroną danych osobowych zgodny z wymaganiami niniejszej Polityki działa z poszanowaniem następujących zasad:

1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2) rzetelnie i uczciwie (rzetelność);
3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
4) w konkretnych celach i nie „na zapas" (minimalizacja);
5) nie więcej niż potrzeba (adekwatność);
6) z dbałością o prawidłowość danych (prawidłowość);
7) nie dłużej niż potrzeba (czasowość);
8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

§ 4

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Jest ona realizowana poprzez: zabezpieczenia fizyczne, zabezpieczenia logiczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
   1) **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   2) **integralność** – rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) **poufność** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
   4) **integralność systemu** – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej jak i przypadkowej.
   5) **dostępność** – gwarantuje, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie.
   6) **uwierzytelnienie** - uwiarygodnienie swojej tożsamości względem systemu teleinformatycznego;
   7) **autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub procesu jest taka, jak deklarowana;
3. Cele i strategie bezpieczeństwa:
   1) zgodność z prawem,
   2) ochrona zasobów informacyjnych i innych aktywów,
   3) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów, rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań,
   4) zapewnienie ciągłości działania procesów i właściwej reakcji na incydenty,
   5) zapewnienie odpowiedniego poziomu wiedzy dotyczącej ochrony danych osobowych wśród pracowników i współpracowników poprzez zapewnienie odpowiednich szkoleń.

§ 5

ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. ADO zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez ADO.
2. ADO przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. *Procedura zarządzania ryzykiem* stanowi **załącznik nr 8** do niniejszej Polityki.
3. Za bezpieczeństwo danych osobowych u ADO odpowiedzialni są wszyscy pracownicy. W szczególności odpowiadają oni za przestrzeganie zasad bezpieczeństwa wynikających z niniejszej Polityki oraz zgłaszanie incydentów i naruszeń, a także wykonywanie zaleceń IOD.
4. We wszystkich umowach, które mogą dotyczyć przetwarzania danych u ADO, należy uwzględnić zapisy zobowiązujące drugą stronę do przestrzegania art. 28 RODO oraz obowiązujących przepisów krajowych.
5. Inspektor ochrony danych prowadzi rejestr podmiotów zewnętrznych, z którymi realizacja umów/porozumień/zamówień lub aneksów do nich zobowiązuje lub umożliwia zleceniobiorcy/wykonawcy dostęp do informacji zawierających dane osobowe.
6. Za przestrzeganie zasad ochrony danych osobowych i za codzienną ochronę danych odpowiedzialni są upoważnieni użytkownicy.

§ 6

Realizację zamierzeń określonych w § 3 powinny zagwarantować następujące założenia:

1) Wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania informacji oraz ich odpowiedzialność za ochronę danych.
2) Przeszkolenie użytkowników w zakresie ochrony danych osobowych.
3) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory).
4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń.
5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych.
6) Opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii.
7) Okresowe aktualizowanie Polityki.
8) Identyfikacja zagrożeń i analiza ryzyka.

II. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH

§ 7

Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, 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.

§ 8

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje to głównie:

1) 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.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy,
3) 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,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur ochrony danych osobowych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.).

§ 9

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

Procedura zgłaszania naruszeń stanowi **załącznik nr 9** do niniejszej Polityki.

III. PRZEDSIĘWZIĘCIA ZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH

§ 10

1. Każdy użytkownik – przed dopuszczeniem do przetwarzania danych osobowych podlega przeszkoleniu z przepisów w tym zakresie oraz wynikających z nich zadań i obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom.
3. Za organizację szkoleń odpowiedzialny jest Inspektor ochrony danych.

§ 11

1. Dla zapewnienia bezpieczeństwa danych zastosowano następujące **środki organizacyjne**:
   1) Dostęp do danych osobowych mogą mieć tylko i wyłącznie użytkownicy posiadający pisemne, imienne upoważnienia nadane przez Administratora Danych.
   2) Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu wszelkich nośników z danymi.
   3) Należy chronić dane przed wszelkim dostępem do nich osób nieuprawnionych.
   4) Pomieszczenia w których są przetwarzane dane osobowe muszą być zamykane na klucz.
   5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy.
   6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora Danych lub IOD.
   7) Dostęp do pomieszczeń w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.
   8) W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
   9) Szafy w których przechowywane są dane powinny być zamykane na klucz.
   10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy.
   11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.
   12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

2. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące **środki techniczne:**
   1) Dostęp do komputerów na których są przetwarzane dane mają tylko upoważnieni pracownicy.
   2) Monitory komputerów na których przetwarzane są dane są tak ustawione aby osoby nieupoważnione nie miały wglądu w dane.
   3) Po zakończeniu pracy komputery przenośne (np. typu notebook) zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach.
   4) W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.
   5) Nie należy udostępniać osobom nieupoważnionym tych komputerów.
   6) W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.
   7) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie) aby nie zostały na nich dane osobowe.
   8) W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.
   9) W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
   10) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
   11) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.
   12) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

IV. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH

§ 12

DZIAŁANIA KORYGUJĄCE I ZAPOBIEGAWCZE

Działania korygujące podejmowane są w przypadku wykrycia niezgodności w działalności, bądź nieprawidłowego działania procesu.

Przesłanką do podjęcia działań korygujących mogą być wyniki kontroli, audytów, zgłoszenia niezgodności, zdarzenia i incydenty związane z ochroną danych osobowych, zapisy, wyniki badania zadowolenia klientów, analiza reklamacji klientów.

Działania zapobiegawcze mają na celu zapobiec wystąpieniu potencjalnych niezgodności.

§ 13

ZGŁASZANIE NARUSZEŃ

ADO stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia – *Instrukcja postępowania w sytuacji zaistnienia naruszenia* stanowi **załącznik nr 9** do niniejszej Polityki.

V. DOSTĘP DO DANYCH OSOBOWYCH

§ 14

1. Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa.
2. W przypadku udostępnienia danych osobowych w celach innych niż włączenie do rejestru, administrator danych udostępnia posiadane informacje osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
3. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony informacji.
5. Przetwarzanie, w tym udostępnianie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celu badań naukowych, dydaktycznych, historycznych oraz statystycznych.
6. Udostępnienie danych może nastąpić jedynie za zgodą Administratora danych lub IOD i powinno być odpowiednio udokumentowane.

§ 15

VI. PRAWA PODMIOTÓW DANYCH

Każdej osobie, której dane osobowe są przetwarzane przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa albo są już zbędne do realizacji celu, dla którego zostały zebrane.
7) *Polityka realizacji praw osób, których dane dotyczą,* sposoby informowania i komunikacji oraz tryb wykonywania praw przez osobę, której dane dotyczą opisane są *w* ***załączniku nr 14*** do niniejszej Polityki.
8) *Procedura udostępniania danych,* stanowi ***załącznik nr 15*** do niniejszej Polityki

§ 16

POROZUMIENIA I KONTAKTY ZE STRONAMI ZEWNĘTRZNYMI.

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, wiążąc podmiot przetwarzający i administratora, określając przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
3. W przypadku zawierania umów z firmami zewnętrznymi mającymi wpływ na funkcjonowanie kluczowych elementów systemu zarządzania bezpieczeństwem informacji zalecane jest zawarcie umowy powierzenia.

ADO przyjął wymagania co do umowy powierzenia przetwarzania danych zawarte we wzorze *umowy powierzenia ogólnej,* stanowiącej **załącznik nr 10** do niniejszej Polityki.

VII. GRUPY INFORMACJI PODLEGAJĄCE OCHRONIE I REJESTR CZYNNOŚCI

§ 17

1. Grupa informacji dotycząca działalności:
   1) dane osobowe ..... (np. uczniów i ich rodziców).

2. Grupa informacji dotycząca pracowników:
   1) prywatne dane osobowe pracowników,
   2) dane osobowe rodzin pracowników,
   3) dane osoby - kandydata do zatrudniania,
   4) informacje dot. obsługi kadrowo-płacowej pracownika (wynagrodzenia, ewidencja czasu pracy, informacja o urlopach) .

3. Grupa informacji dotycząca infrastruktury fizycznej i teleinformatycznej:
   1) dane o zabezpieczeniach systemu informatycznego,
   2) dane o zabezpieczeniach infrastruktury fizycznej,
   3) informacje dotyczące systemów zarządzania
   4) dokumentacja techniczna infrastruktury.

4. **Rejestr czynności przetwarzania danych osobowych** (RCPDO) stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli **zasady rozliczalności**.

5. W Rejestrze, dla każdej czynności przetwarzania danych, którą ADO uznał za odrębną odnotowuje co najmniej: (1) nazwę czynności, (2) cel przetwarzania, (3) opis kategorii osób i opis kategorii danych, (5) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu ADO, jeśli podstawą jest uzasadniony interes, (6) Ź, (7) opis kategorii odbiorców danych (w tym przetwarzających), (8) informację o przekazaniu poza EU/EOG; (9) ogólny opis technicznych i organizacyjnych środków ochrony danych.

6. Inspektor ochrony danych monitoruje prowadzenie Rejestru czynności przetwarzania danych osobowych. Wzór *Rejestru czynności przetwarzania* stanowi **załącznik nr 4** do niniejszej Polityki.

VIII. BEZPIECZEŃSTWO OSOBOWE

§ 18

ETAP NABORU PRACOWNIKA I WSPÓŁPRACOWNIKA

1. Do przetwarzania danych osobowych i do dostępu do innych informacji chronionych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Administrator danych może wydać pełnomocnictwo do nadawania upoważnień.
2. Wzór *upoważnienia do przetwarzania danych osobowych* stanowi **załącznik nr 6** do niniejszej Polityki. Upoważnienia rejestruje się w *ewidencji upoważnień*, stanowiącej **załącznik nr 12** do niniejszej Polityki.
3. Zakres upoważnienia może również być określony w umowie o pracę lub współpracę.
4. Osoba upoważniona zobowiązana jest podpisać oświadczenie lub umowę, która określa odpowiedzialność w zakresie ochrony danych osobowych.
5. Osoby upoważnione do przeprowadzania działań związanych z naborem powinny zwrócić szczególną uwagę na zasady ochrony danych wymienione w § 3 niniejszej Polityki, a także aktualnie obowiązujące przepisy prawa w tym zakresie.

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH

1. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych nadzoruje Inspektor Ochrony Danych. Wzór ewidencji stanowi **załącznik nr 12** do niniejszej Polityki.

2. Ewidencja zawiera:
   1) imię i nazwisko użytkownika,
   2) datę nadania i ustania upoważnienia
   3) zakres upoważnienia
   4) identyfikator użytkownika

3. Ewidencja użytkowników może być prowadzona w systemie informatycznym.

4. Zmiany dotyczące użytkownika, takie jak:
   1) zmiana imienia lub nazwiska,
   2) zmiana zakresu upoważnienia,

   podlegają niezwłocznemu odnotowaniu w ewidencji.

5. Zmiany dotyczące użytkownika, takie jak:
   1) rozwiązanie umowy,
   2) utrata upoważnienia do przetwarzania danych osobowych
   3) zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia, powodują wyrejestrowanie użytkownika przez Administratora Aplikacji oraz ASI w trybie natychmiastowym z ewidencji, zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.

6. Osoba odpowiedzialna za sprawy kadrowe, bezpośredni przełożony Użytkownika, odpowiadają za natychmiastowe zgłoszenie do ASI użytkowników, którzy utracili uprawnienia do dostępu do danych osobowych, celem zablokowania im dostępu do systemu informatycznego poprzez zablokowanie identyfikatora i wyrejestrowanie z ewidencji osób upoważnionych.

7. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.

§ 19

ZATRUDNIENIE / WSPÓŁPRACA

1. Pracownicy, współpracownicy, wykonawcy i podwykonawcy powinni być świadomi swoich obowiązków i odpowiedzialności prawnej oraz zagrożeń związanych z bezpieczeństwem informacji. W tym celu należy zapewnić wszystkim zatrudnionym właściwy poziom świadomości poprzez kształcenie i szkolenie z zakresu ochrony danych osobowych, ze szczególnym uwzględnieniem procedur bezpieczeństwa. Dokumentują to:
   - lista obecności ze szkoleń,
   - oświadczenia pracowników,
   - umowy o poufności
   - posiadane zaświadczenia, dyplomy lub certyfikaty.
2. W przypadku naruszenia zasad ochrony danych osobowych jest uruchomiana odpowiednia procedura postępowania dyscyplinarnego, która powinna być poprzedzona potwierdzeniem naruszenia zasad ochrony danych osobowych i zgromadzeniem materiału dowodowego.
3. Postępowanie dyscyplinarne powinno uwzględniać: rodzaj i wagę naruszenia zasad ochrony danych osobowych, wpływ na procesy biznesowe, przypadek incydentalny czy jest to kolejne naruszenie oraz jakość odbytego przeszkolenia.
4. W przypadku pracy mobilnej i na odległość z wykorzystaniem urządzeń przenośnych zastosowano odpowiednie, dodatkowe środki bezpieczeństwa.
5. Przekazywanie sprzętu i urządzeń służących do przetwarzania danych odbywa się na podstawie protokołów przekazania sprzętu.

§ 20

ZAKOŃCZENIE ZATRUDNIENIA / WSPÓŁPRACY

1. Zakończenie zatrudnienia lub zmiana stanowiska pracy wewnątrz organizacji powinny odbywać się w sposób zorganizowany.
2. Odchodzenie z organizacji lub zmiana stanowiska pracy wiąże się ze zwrotem posiadanego przez pracownika sprzętu i odebraniem lub zmianą praw dostępu.
3. Odebranie lub ograniczenie praw dostępu jest poprzedzone analizą ryzyka uwzględniającą następujące uwarunkowania:
   1) ustalenie inicjatora (pracownik, wykonawca czy kierownictwo ADO) i przyczyn zakończenia lub zmiany zatrudnienia;
   2) aktualny zakres czynności pracownika, wykonawcy lub podwykonawcy;
   3) wartość aktualnie dostępnych aktywów.

§ 21

ZASADY PRZYZNAWANIA DOSTĘPU

1. Przyznawanie zakresu uprawnień powinno być w ścisłym związku z zakresem obowiązków danego pracownika.
2. Zarządzanie dostępem na etapie nadawania, zmiany i cofania praw dostępu pracowników w obszarze przetwarzania danych oraz do systemów teleinformatycznych powinno się odbywać na wniosek bezpośredniego przełożonego Użytkownika.
3. W zarządzaniu dostępem obowiązuje zasada, że dostęp użytkownika powinien opierać się na spełnieniu zasady rozliczalności oraz zasady niezaprzeczalności. W przypadku systemów informatycznych obowiązują następujące wymagania:
   1) wymóg jednoznacznej identyfikacji pracownika - tj. w systemach informatycznych każdy użytkownik pracuje wyłącznie na swoim indywidualnym koncie, nie są stosowane konta anonimowe lub współdzielone poza wyjątkami, gdzie z przyczyn technicznych nie ma innej możliwości,
   2) wymóg uwierzytelnienia pracownika przy korzystaniu z systemu informatycznego,
   3) autoryzacji przyznania praw dostępu do systemów informatycznych.
   4) zasady przywilejów, wiedzy i usług koniecznych.

IX. BEZPIECZENSTWO TELEINFORMATYCZNE

§ 22

AUTORYZACJA I DOPUSZCZALNE WYKORZYSTANIE ZASOBÓW.

1. Przy ochronie zasobów kluczowe jest stosowanie podstawowej zasady bezpieczeństwa, że nie jest dozwolone wykorzystywanie zasobów w sposób inny niż jawnie dozwolony.
2. Do wykonywania obowiązków służbowych związanych z przetwarzaniem informacji dozwolone jest używanie systemów, urządzeń i oprogramowania dopuszczonych do użytku zgodnie z wymogami Polityki
3. Pracownicy są uprawnieni do korzystania z zasobów teleinformatycznych niezbędnych do wykonywania ich obowiązków. Szczegółowa *procedura przyznawania dostępu wynika z instrukcji zarządzania systemem informatycznym* i stanowi **załącznik nr 11** do niniejszej Polityki.
4. Zakazane jest użytkowanie na terenie obszaru przetwarzania danych lub przy wykonywaniu obowiązków służbowych poza obszarem przetwarzania danych innych niż dopuszczone urządzeń, systemów i oprogramowania bez zgody Administratora Systemu Informatycznego (ASI).
5. Zakazane jest bez zgody ASI:
   a) użytkowanie urządzeń skutkujących połączeniem systemów Administratora danych z sieciami teleinformatycznymi innych podmiotów, w tym publicznymi sieciami teleinformatycznymi,
   b) użytkowanie urządzeń lub oprogramowania mających na celu zakłócenie działania innych systemów, urządzeń lub oprogramowania,
   c) użytkowanie urządzeń lub oprogramowania do testowania bezpieczeństwa lub wykrywania podatności,
   d) użytkowanie urządzeń lub oprogramowania mogących naruszyć bezpieczeństwo innych systemów lub urządzeń,

e) wprowadzanie zmian konfiguracji urządzeń, systemów lub oprogramowania.

6. Zakazane jest bez zgody IOD wykorzystywanie urządzeń do niejawnego przekazywania lub rejestracji danych dotyczących informacji chronionych, w tym głosu i obrazu, tj.: magnetofonów, dyktafonów, aparatów fotograficznych, kamer, telefonów komórkowych z opcją rejestrowania dźwięku i obrazu, rejestratorów ruchu sieciowego, rejestratorów pracy klawiatur itp.
7. Powyższy zakaz nie dotyczy sytuacji, gdy rejestrowane są dane pochodzące z systemu testowego, a działania pracownika nie prowadzą, i w sposób oczywisty nie mogą prowadzić, do odczytywania jakichkolwiek poufnych informacji, do których pracownik nie ma dostępu.
8. Wykorzystanie należących do Administratora danych urządzeń, systemów i oprogramowania oraz innych zasobów do prywatnych celów pracowników jest dozwolone jedynie na uzasadniony wniosek pracownika i za zgodą IOD i ASI.
9. Zasoby Administratora danych powinny być przechowywane w taki sposób, aby zapobiec możliwości ich kradzieży lub uszkodzenia przez osoby postronne oraz przypadkowe uszkodzenia przez osoby lub czynniki środowiskowe.
10. Wynoszenie aktywów (zasobów i informacji) poza obszar przetwarzania danych możliwe jest za zgodą IOD lub ADO.
11. Zakazane jest przesyłanie informacji podlegających ochronie na prywatne adresy poczty elektronicznej oraz prowadzenie korespondencji służbowej z wykorzystaniem prywatnego adresu e-mail użytkownika.
12. Zakazane jest używanie prywatnych nośników zewnętrznych (np. typu pendrive) i tworzenie nieautoryzowanych kopii z baz danych.
13. Pracownicy zobowiązani są stosować zasadę czystego biurka i ekranu - wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szafkach, szufladach itp. W przypadku braku dostatecznej ilości dostępnego miejsca dokumenty i materiały powinny być pozostawiane na biurku uporządkowane.
14. Pracownicy są zobowiązani do ochrony zasobów będących własnością innych podmiotów, a powierzonych lub oddanych do dyspozycji Administratorowi danych lub udostępnionych pracownikom na czas wykonywania przez nich czynności służbowych w takim samym stopniu jak w przypadku zasobów będących własnością Administratora danych.
15. Procedury i instrukcje dotyczące bezpieczeństwa teleinformatycznego opracowuje ASI i przechowuje w Teczce ODO.

§ 23

METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Identyfikator

1) Identyfikator nadaje Administrator Sytemu Informatycznego lub Administrator Aplikacji.
2) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

2. Hasło użytkownika

1) Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.
2) Użytkownicy powinni stosować hasła, które:

a) są łatwe do zapamiętania, a trudne do odgadnięcia,
b) nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.),
c) zawierają przynajmniej jedną dużą literę, jedną małą literę, jedną cyfrę lub znak specjalny.

3) Hasła powinny być często zmieniane, na przykład co 30 dni; IOD lub ASI może, w uzasadnionych sytuacjach polecić dokonanie zmiany hasła przez użytkownika np. po każdym incydencie lub podejrzeniu naruszenia bezpieczeństwa.
4) Należy unikać ponownego lub cyklicznego używania starych haseł.
5) Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.
6) Pracownicy są odpowiedzialni za zachowanie w poufności swoich haseł.
7) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).
8) Użytkownik wprowadza swoje hasło w sposób uniemożliwiający innym osobom jego poznanie.
9) W sytuacji, gdy zachodzi podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik natychmiast dokonuje zmiany hasła.
10) Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
11) Administrator Systemu Informatycznego oraz Specjalista ds. odo przeprowadzają okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach za które są odpowiedzialni.

3. Hasło administratora systemu informatycznego

Hasła użytkowników uprzywilejowanych (tzn. użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych) są zabezpieczone u Administratora danych na wypadek sytuacji awaryjnych, szczególnie w przypadku nieobecności administratora systemu.

X. POSTANOWIENIA KOŃCOWE

§ 24

1. Do stosowania zasad określonych przez dokumenty Polityki zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy i inne osoby mające dostęp do informacji podlegającej ochronie.
2. Z treścią niniejszego dokumentu powinni zapoznać się wszyscy pracownicy i inne osoby mające dostęp do informacji przetwarzanej u ADO, przed przystąpieniem do przetwarzania danych.
3. Niniejszy dokument może być przedstawiany podmiotom i jednostkom współpracującym z którymi współpraca może skutkować możliwością dostępu do informacji chronionych.
4. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a

także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne lub porządkowe.

5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym IOD.
6. W przypadku naruszenia postanowień Polityki pracownik, który dopuścił się takiego naruszenia lub przyczynił do niego (umyślnie lub nieumyślnie) może zostać ukarany zgodnie z obowiązującym regulaminem pracy, obowiązującymi przepisami prawa z zakresu ochrony danych osobowych, a w skrajnych przypadkach pociągnięty do odpowiedzialności karnej.
7. Umyślne lub nieumyślne naruszenie postanowień Polityki lub niestosowanie się do poleceń służbowych w tym zakresie może być potraktowane jako naruszenie obowiązków pracowniczych.

§ 25

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
2. Użytkownicy są zobowiązani zapoznać się z treścią Polityki
3. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami i zasadami z zakresu ochrony danych osobowych, z niniejszą Polityką, a także zobowiązać się do ich przestrzegania.
4. Wzór *oświadczenia* potwierdzającego zaznajomienie użytkownika z przepisami w zakresie ochrony informacji oraz z dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania, stanowi **załącznik nr 5** do niniejszej Polityki.
5. Oświadczenia przechowywane są w aktach osobowych.

§ 26

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych, szczególnie RODO.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania postanowień zawartych w niniejszej Polityce. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

XI. SPIS ZAŁĄCZNIKÓW

1. Wyznaczenie i obowiązki IOD - załącznik nr 1
2. Wyznaczenie Administratora Systemu Informatycznego - załącznik nr 2
3. Obszar przetwarzania danych – środki bezpieczeństwa - załącznik nr 3
4. Rejestr czynności przetwarzania - załącznik nr 4
5. Oświadczenie użytkownika – załącznik nr 5
6. Upoważnienie do przetwarzania danych osobowych - załącznik nr 6
7. Plan audytu i przeglądów Polityki ochrony danych osobowych – załącznik nr 7
8. Procedura zarządzania ryzykiem – załącznik nr 8
9. Instrukcja postępowania w sytuacji zaistnienia naruszenia– załącznik nr 9
10. Wzór umowy powierzenia przetwarzania danych - załącznik nr 10
11. Instrukcja zarządzania systemem informatycznym - załącznik nr 11
12. Ewidencja osób upoważnionych – wzór - załącznik nr 12
13. Regulamin IOD – załącznik nr 13
14. Polityka realizacji praw osób, których dane dotyczą, sposoby informowania i komunikacji oraz tryb wykonywania praw przez osobę, której dane dotyczą – załącznik nr 14
15. Procedura udostępniania danych – załącznik nr 15

załącznik nr 1

WYZNACZENIE I OBOWIĄZKI INSPEKTORA OCHRONY DANYCH

Na podstawie art. 37 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. Nr 119, str. 1) oraz art. 8 Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2018 r. poz. 1000)

Wyznacza się: **Pana Tomasza Pilch** prowadzącego działalność gospodarczą pod nazwą:
FIRMA USŁUGOWA SZKOLENIA I DORADZTWO PILCH TOMASZ,
Szerzyny 585, 38-246 Szerzyny, NIP: 873-169-29-04

Do pełnienia funkcji: **Inspektora Ochrony Danych**

W podmiocie o nazwie: ***Szkoła Podstawowa nr 2 w Woli Rzędzińskiej,***
33-150 Wola Rzędzińska 253 A

Zadania Inspektora Ochrony Danych określa art. 39 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)

OŚWIADCZENIE INSPEKTORA OCHRONY DANYCH

Oświadczam, że przyjmuje powierzoną funkcję, zapoznałem się z obowiązkami Inspektora Ochrony Danych. Ponadto jako **Inspektor Ochrony Danych**, będę nadzorował przestrzeganie zasad ochrony danych w podmiocie o nazwie: ***Szkoła Podstawowa nr 2 w Woli Rzędzińskiej,*** zgodnie z obowiązkami wynikającymi z ustawy o ochronie danych osobowych oraz RODO.
Oświadczam, że spełniam wymogi dotyczące osoby powołanej na stanowisko:
INSPEKTORA OCHRONY DANYCH.

Administrator Danych Osobowych	**Inspektor Ochrony Danych**
----------	----------
Podpis	**Podpis**

załącznik nr 2

Wola Rzędzińska, dn. .....

POWOŁANIE
funkcji Administratora Systemów Informatycznych
w ***Szkole Podstawowej nr 2 w Woli Rzędzińskiej***

Na podstawie wprowadzonej Polityki Bezpieczeństwa Informacji oraz 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, zwane dalej RODO, powołuję Panią/Pana:

…….

na funkcję Administratora Systemów Informatycznych

Tym samym powierzam Pani/Panu zadania związane z utrzymaniem ciągłości działania oraz bezpieczeństwa w infrastrukturze informatycznej. Jest Pani/Pan także zobowiązany do inwentaryzowania oraz okresowego sprawdzenia stanu urządzeń oraz sprzętu pozwalającego na obsługę czynności przetwarzania danych osobowych w systemach informatycznych.

Informuję Panią/Pana, iż w ramach powierzonych obowiązków jest Pani/Pan uprawniona/y do:

1. wstępu do pomieszczeń, w których znajdują się urządzenia infrastruktury informatycznej,
2. odbierania wyjaśnień od osób przetwarzających dane osobowe,
3. dokumentowania ustaleń i dokonywania innych czynności niezbędnych do wykonania zadań wynikających niniejszego upoważnienia.

OŚWIADCZENIE ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Niniejszym zobowiązuję się do zachowania poufności, nieujawniania osobom nieupoważnionym i zachowania w tajemnicy wszelkich danych z którymi mam styczność podczas wykonywania powierzonych mi zadań, a dane te nie są danymi publicznymi.
Potwierdzam, że zapoznałem się z Polityką Bezpieczeństwa Informacji oraz wszelkimi regulacjami i procedurami z tego zakresu, wprowadzonymi przez Administratora Danych.

....

data i podpis ASI ***podpis ADO***

załącznik nr 3

I. OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH – środki bezpieczeństwa

1. Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemie informatycznym.

2. Dane osobowe przetwarzane są na terenie szkoły.

3. Ze względu na nagromadzenie danych osobowych szczególnie chronione powinny być pomieszczenia, zgodnie z poniższym wykazem.

Budynek	Rodzaj dokumentów	Miejsce przechowywania
Budynek szkoły	Dzienniki lekcyjne (oddział przedszkolny, przedszkole)	
	Dzienniki zajęć specjalistycznych	
	Zeszyty wychowawcy	
	Dzienniki zajęć pozalekcyjnych	
	Dzienniki świetlicy	
	Dziennik pedagoga	
	Dziennik bibliotekarza	
	Księga ewidencji uczniów	
	Księga uczniów	
	Arkusze ocen	
	Dokumenty z nadzoru pedagogicznego	
	Dokumentacja pomocy pp	
	Ewidencja uczniów przystępujących do egzaminu zewnętrznego	
	Dokumentacja opiekuńczo-wychowawcza	
	Arkusz organizacyjny szkoły	
	Dokumentacja ZFŚS	
	Postępowanie administracyjne w sprawie realizacji obowiązku nauki	
	Decyzje o odroczenie obowiązku szkolnego	
	Podania ubiegających się o pracę	
	Ewidencja wydanych świadectw, zaświadczeń i legitymacji	
	Księga kontroli zewnętrznej	
	Lista obecności	
	Dziennik korespondencyjny	
	Rejestr upoważnień	
	protokoły wypadkowe	

	Dokumenty archiwalne	
	Lokalne bazy SIO – uczniowie i budynki	
	Teczki awansu zawodowego	
	Akta osobowe	
	Listy płac	
	Dokumentacja Komisji Zdrowotnej	
	Dokumentacja kadrowa	
	Lokalne bazy SIO - sprawy kadrowe	

załącznik nr 4

Rejestr czynności przetwarzania w jednostkach oświatowych

ADMINISTRATOR DANYCH	
Nazwa	Administratorem przetwarzanych danych osobowych jest : ***Szkoła Podstawowa nr 2 im. Edmunda Bojanowskiego w Woli Rzędzińskiej*** reprezentowane przez dyrektora jednostki
Adres	***33-150 Wola Rzędzińska 253 A***
Numer telefonu	***14 679 21 24***
Adres poczty elektronicznej	***kontakt@szpwola.pl***
INSPEKTOR OCHRONY DANYCH	
Imię i nazwisko	***Tomasz Pilch***
Numer telefonu	***782 974 835***
Adres poczty elektronicznej	***firma.tomaszpilch@onet.pl***

Nr wpisu w rejestrze	
Cel przetwarzania	
Podstawa przetwarzania	
Opis kategorii osób	
Kategorie danych osobowych	
Kategorie odbiorców danych	
Planowany termin usunięcia danych	
Współadministratorzy	
Informacje o przekazaniu do państwa trzeciego	
Opis technicznych środków bezpieczeństwa	

Załącznik nr 5

Wola Rzędzińska, dnia .....

.....
Imię i nazwisko

Oświadczenie o zapoznaniu się z treścią
Polityki Ochrony Danych Osobowych
obowiązującej
w Szkole Podstawowej nr 2 w Woli Rzędzińskiej

Oświadczam, że zapoznałam(-łem) się z treścią Polityki ochrony danych osobowych i zobowiązuję się do przestrzegania zawartych w tym dokumencie zasad, reguł i postanowień.

.....
Data i podpis

Załącznik nr 6

Numer upoważnienia: ***……/……..*** Wola Rzędzińska, dn…… r.

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO –** nadaję upoważnienie Pani:

……..
(imię i nazwisko)

……
(stanowisko)

do przetwarzania danych osobowych w zakresie zawartym w zbiorach:

……

……

…….

Jednocześnie zobowiązuję Panią do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, a także z Polityką ochrony danych osobowych Pracodawcy.

Jednocześnie upoważniam Panią do tworzenia dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w:

Szkole Podstawowej nr 2 w Woli Rzędzińskiej

Okres ważności
od: ***…….***
do: ***czasu rozwiązania umowy z pracodawcą.***

……

podpis osoby uprawnionej do nadania upoważnienia

Oświadczam, że:

- otrzymałem(am) niniejsze upoważnienie, zrozumiałem(am) jego treść i w pełni akceptuję zakres moich obowiązków służbowych dotyczących przetwarzania danych osobowych powierzonych mi przez administratora i zobowiązuję się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz do zachowania klauzuli poufności dotyczącej przetwarzanych danych osobowych powierzonych mi przez administratora,

- zostałem(am) zapoznany(a) z przepisami o ochronie danych osobowych, 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) oraz Polityką Ochrony Danych obowiązującą w Szkole Podstawowej nr 2 w Woli Rzędzińskiej.

- zostałem(am) poinformowany/a o grożącej, stosownie do przepisów o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Przyjęto do wiadomości i stosowania

……..
data i podpis pracownika

Data wygaśnięcia* ……..

Odwołano, dnia …….

……..
podpis osoby uprawnionej do odwołania upoważnienia

Załącznik nr 7

Plan wewnętrznego audytu i przeglądów polityk bezpieczeństwa danych osobowych

1. Plan kontroli wewnętrznej obejmuje następujące zagadnienia:
   1.1. funkcjonowanie zabezpieczeń systemowych,
   1.2. prawidłowość funkcjonowania mechanizmów dostępu do zbiorów danych
   1.3. funkcjonowanie zastosowanych zabezpieczeń fizycznych,
   1.4. zasady przechowywania kartotek,
   1.5. zasady i sposoby likwidacji oraz archiwizowania zbiorów archiwalnych,
   1.6. realizacja procedur wdrożonych przez Administratora Danych w zakresie ochrony danych osobowych,
2. Zagadnienia, czynności kontrolno-oceniające ujęte są w harmonogramie ich przeprowadzania, ze wskazaniem osób je wykonujących.
3. Dodatkowe czynności kontrolne potwierdzone są w zakresie zadań, kompetencji i odpowiedzialności tych pracowników, którzy takie uprawnienia z relacji zajmowanych stanowisk posiadają.
4. Za zorganizowanie i prawidłowe działanie kontroli wewnętrznej, a także za należyte wykorzystanie wyników kontroli odpowiedzialny jest Inspektor ochrony danych.
5. Z kontroli wewnętrznej kontrolujący sporządza pisemną notatkę. Z wynikami kontroli zapoznaje kontrolowane strony i Administratora danych

ANALIZA ORGANIZACYJNYCH ŚRODKÓW BEZPIECZEŃSTWA INFORMACJI

L.P.	ZAGADNIENIA / OBOWIĄZUJĄCE WYMAGANIA / ZAKRES KONTROLI	REKOMENDACJE / ZALECENIA	STAN FAKTYCZNY / UWAGI / ZALECANE ROZWIĄZANIA	DATA, IMIĘ, NAZWISKO lub STANOWISKO OSOBY KONTROLUJĄCEJ LUB ODPOWIEDZIALNEJ
1.	Analiza i aktualizacja Polityki ochrony danych osobowych. Sprawdzenie jej zgodności z aktualnymi przepisami.	Przegląd dokumentacji powinien odbywać się nie rzadziej niż raz na rok		
2.	Przeprowadzić inwentaryzację aktywów w zakresie informacji mających wartość dla Administratora danych.	Wskazać grupy informacji podlegających ochronie. Sprawdzić aktualność Rejestru czynności przetwarzania danych osobowych.		
3.	Sprawdzenie zakresu, rodzaju zbieranych danych, celów w jakich są zbierane i adekwatności.	Sprawdzenie zasady celowości, adekwatności, merytorycznej poprawności oraz ograniczenia czasowego		
4.	Podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji	Sprawdzenie sposobu nadawania upoważnień do przetwarzania danych oraz ich zakresu. Sprawdzenie aktualności i sposobu prowadzenia Ewidencji osób upoważnionych do przetwarzania danych. Oświadczenia o zachowaniu tajemnicy. Polityka lub procedura nadawania dostępów w systemach informatycznych.		
5.	Sprawdzenie treści klauzul informacyjnych.	Sposób realizacji obowiązku informacyjnego z uwzględnieniem szczególnych przepisów prawa.		
6.	Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji	Sprawdzenie umów z zewnętrznymi firmami pod kątem potrzeby zawarcia umów powierzenia. Ewidencja podmiotów zewnętrznych.		
7.	Zapewnienie szkolenia osób zaangażowanych w proces przetwarzania	Szkolenia stanowiskowe. Karty szkoleniowe.		

	informacji	Oświadczenia pracowników. Szkolenia z udziałem zewnętrznych specjalistów.		
8.	Opis i zabezpieczenie obszaru przetwarzania danych.	Wykaz pomieszczeń, w których przetwarzane są dane osobowe. Gospodarka kluczami. Fizyczne środki bezpieczeństwa (kraty, alarmy, monitoring itp.)		
9.	Sposoby zabezpieczenia danych przetwarzanych w formie papierowej.	Zasada „czystego biurka”. Zamykane metalowe i niemetalowe szafy. Sposoby przechowywania kluczy do szaf. Niszczarki dokumentów.		
10.	Zabezpieczenia przed skutkami pożaru	Systemy gaszenia pożaru lub wolnostojące, odpowiednie gaśnice. Plany ewakuacji, wyznaczone miejsca zbiórki dla ludzi i sprzętu. Przechowywanie kopii bezpieczeństwa w innej lokalizacji.		
11.	Procedura oceny i zgłoszenia naruszenia bezpieczeństwa danych osobowych.	Instrukcja postępowania w przypadku naruszenia ochrony danych. Formularze do zgłoszenia naruszenia bezpieczeństwa.		
12.	Realizacja praw podmiotów danych, tj. osób, których dane dotyczą.	Procedury udzielania informacji o zakresie przysługujących praw.		
ANALIZA TECHNICZNYCH I INFORMATYCZNYCH ŚRODKÓW BEZPIECZEŃSTWA INFORMACJI				
13.	Tryb i częstotliwość tworzenia kopii zapasowych	Procedury wykonywania i odtwarzania kopii zapasowych. Przechowywanie kopii w innej lokalizacji. Testowanie kopii – protokoły z testowania		
14.	Plany ciągłości działania systemów	Plan odbudowy oprogramowania po awarii		

	informatycznych w przypadku wystąpienia awarii katastrofalnej.	Plan utrzymania ciągłości działania Systemów informatycznych		
15.	Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację	Raport z inwentaryzacji komputera Raport podsumowywujący inwentaryzację oprogramowania Rejestr komputerów przenośnych.		
16.	Dziennik Administratora systemu informatycznego. Rejestr incydentów	Dokumentowanie czynności z zakresu eksploatacji, aktualizacji i monitoringu systemu i oprogramowania. Protokoły z naruszenia ochrony danych. Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych		
17.	Proces uwierzytelniania i identyfikacji użytkowników w systemie	Konta użytkowników i loginy. Polityka haseł. Identyfikacja osób dokonujących wpisu.		
18.	Rozliczalność w systemach teleinformatycznych	Historia logów		
19.	Bezzwłoczna zmiana uprawnień w przypadku zmiany zadań osób upoważnionych lub ustania upoważnienia	Blokowanie haseł i kont byłego pracownika. Zwrot sprzętu i innych aktywów		
20.	Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji	Badanie podatności i wykrywanie słabych punktów systemu i stron www. Aktualizacja oprogramowania, w tym antywirusowego.		
21.	Środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity	Legalność i aktualność programu antywirusowego. Firewall do ochrony dostępu do sieci komputerowej. System IDS/IPS		
22.	Zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na	Ewidencja laptopów. Hasła na BIOS lub programy szyfrujące.		

	odległość	Szyfrowane połączenia i protokoły.		
23.	Minimalizowanie ryzyka utraty informacji w wyniku awarii	UPS, generator prądu itp. Listwy przepięciowe. Kopie zapasowe.		
24.	Ochrona przed błędami, utratą, nieuprawnioną modyfikacją	Integralność danych i systemów jako brak możliwości nieuprawnionych zmian, kopiowania, usuwania.		
25.	Stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa	Szyfrowany protokół SSL VPN Bezpieczeństwo sieci		
26.	Mechanizmy automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika	Wygaszacze ekranów zabezpieczone hasłem. Blokowanie stanowiska pracy.		
27.	Zasady bezpiecznego korzystania z Internetu i poczty elektronicznej	Blokowanie zbędnych i groźnych stron i treści. Monitoring sieci i poczty.		
28.	Zabezpieczenie serwerowni	Wydzielenie pomieszczenia. System kontroli dostępu. Klimatyzacja lub pomiar temperatury i wilgotności.		
29.	Bezpieczeństwo danych na dyskach i innych nośnikach informacji przeznaczonych do naprawy lub likwidacji	Pozbawianie lub uszkadzanie zapisu danych Nadzór osób upoważnionych. Umowy powierzenia. Protokoły i raporty usuwania danych.		
30.	Bezpieczeństwo i zasady współpracy z podmiotami zewnętrznymi np. dostawcami lub serwisantami oprogramowania czy serwerów.	Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji		

Załącznik nr 8

Procedura zarządzania ryzykiem w obszarze ochrony danych osobowych:

Ogólne zasady zarządzania ryzykiem 1

Identyfikacja ryzyka 2

Analiza ryzyka 2

Przykłady zagrożeń, ryzyk, następstw 3

Prawdopodobieństwo wystąpienia ryzyka 4

WYTYCZNE DO OCENY PRAWDOPODOBIEŃSTWA WYSTĄPIENIA I NASTĘPSTW RYZYKA 5

Następstwo (wpływ) 7

Istotność 7

Reakcja na ryzyko i działania zaradcze 7

Rejestry ryzyk 9

Załącznik nr 1 do Procedury Zarządzania Ryzykiem - szacowanie ryzyka / wzór / 01

Załącznik nr 2 "Mapa ryzyka" / wzór / 11

Postanowienia ogólne

§ 1.

Polityka zarządzania ryzykiem w obszarze ochrony danych osobowych u **Administratora danych osobowych** opisuje model zarządzania ryzykiem oraz określa jego ogólne zasady.

Ogólne zasady zarządzania ryzykiem

§ 2.

1. Zarządzanie ryzykiem w kontekście ochrony danych osobowych jest procesem ciągłym.

2. Celem zarządzania ryzykiem jest wdrożenie odpowiednich środków technicznych i organizacyjnych w taki sposób, aby przetwarzanie danych odbywało się zgodnie z RODO (ROZPORZĄDZENIEM PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

3. Zarządzanie ryzykiem powinno prowadzić do eliminacji lub ograniczenia - do akceptowanego poziomu - prawdopodobieństwa i następstw wystąpienia zdarzeń negatywnych.

4. Ilekroć w niniejszej procedurze jest mowa o:

1) **analizie ryzyka** - rozumie się przez to identyfikowanie i opisywanie ryzyka oraz oszacowanie wielkości jego następstw i prawdopodobieństwa przy uwzględnieniu skuteczności istniejących zabezpieczeń, zastosowanych organizacyjnych, logicznych i technicznych środków bezpieczeństwa,
2) **następstwach, skutkach naruszenia praw lub wolności dla osób fizycznych** - zidentyfikowane reakcje dla określonych procesów przetwarzania danych (np.: kradzież tożsamości),
3) **organizacyjnych i technicznych środkach bezpieczeństwa, mechanizmach kontrolnych** - rozumie się przez to polityki, zarządzenia, procedury, instrukcje, praktyki, fizyczne i techniczne środki zabezpieczeń, systemy, zaprojektowane i wdrożone w celu ograniczenia prawdopodobieństwa wystąpienia i/lub następstw ryzyka; podstawowy zestaw mechanizmów kontrolnych, nie stanowiący katalogu zamkniętego,
4) **procesie** - rozumie się przez to ciąg czynności zaprojektowanych, a następnie wykonywanych w ten sposób, aby w ich wyniku powstał produkt lub usługa,
5) **rejestrze ryzyka** - rozumie się przez to zestawienie zawierające informacje o wyniku przeprowadzonej identyfikacji i oceny ryzyka, a także zaproponowanej reakcji na ryzyko,
6) **ryzyku** - rozumie się przez to zagrożenie związane ze zdarzeniem lub działaniem, które wpłynie na zdolność organizacji do realizacji skutecznej ochrony danych,
7) **właścicielu ryzyka** - rozumie się przez to podmiot odpowiedzialny za zarządzanie danym ryzykiem; właścicielem ryzyka w organizacji jest Administrator danych lub właściciel procesu odpowiedzialny za realizację procesu, do którego odnosi się to ryzyko,
8) **zarządzaniu ryzykiem** - rozumie się przez to działania podejmowane w celu

identyfikacji, oceny, określenia reakcji na ryzyko, a także skoordynowanych działań dotyczących jego minimalizacji.

Identyfikacja ryzyka

§ 3.

1. Identyfikacja ryzyka polega na rozpoznaniu, określeniu i opisaniu ryzyk, które mogą wystąpić jako przeszkody w realizacji zadań/procesów związanych z ochroną danych.
2. W procesie identyfikacji ryzyka uwzględnia się zagrożenia związane z wystąpieniem jakiegokolwiek zdarzenia, działania lub braku działania, które może mieć negatywny wpływ dla osób fizycznych, których dane są przetwarzane w organizacji.
3. Podczas identyfikacji należy odnieść się w szczególności do:
   1) procesów dotyczących przetwarzania danych osobowych,
   2) celu przetwarzania danych osobowych,
   3) kategorii osób, których dane dotyczą,
   4) zakresu danych identyfikujących osobę fizyczną,
   5) możliwości przetwarzania danych szczególnie chronionych,
   6) odbiorców danych i sposobów wykorzystywania przez nich danych z uwzględnieniem ujawnianego ich zakresu,
   7) okresu retencji danych.
4. Identyfikacja ryzyka powinna prowadzić do możliwie dokładnego ustalenia charakteru ryzyka i jego zakresu, co umożliwi wybór i podjęcie we właściwym czasie odpowiednich czynności zapobiegawczych bądź też ograniczających wpływ ryzykownych działań.
5. Identyfikacja powinna uwzględniać ryzyko znane powszechnie oraz nowo identyfikowane - aktualizowane.
6. Identyfikacji podlega zarówno ryzyko wewnętrzne, mające swoje źródło w działaniach podejmowanych przez pracowników organizacji, jak i ryzyko zewnętrzne, wynikające z czynników zewnętrznych.
7. Identyfikacja ryzyka powinna uwzględniać wyniki z przeprowadzonych w organizacji audytów i kontroli: zarówno wewnętrznych, jak i zewnętrznych.

Analiza ryzyka

§ 4.

1. Wszystkie zidentyfikowane rodzaje ryzyka poddawane są całościowej analizie.
2. Proces analizy ryzyka ma charakter subiektywnej oceny dokonywanej przez osoby uprawnione do analizy ryzyka.
3. Ocena poszczególnych rodzajów ryzyka odbywa się w oparciu o przyjęty w Procedurze model oceny ryzyka, zapewniający porównywalność wyników we wszystkich obszarach funkcjonowania organizacji oraz ułatwiający przetwarzanie i łączenie indywidualnych ocen w celu stworzenia ogólnego profilu ryzyka.
4. Celem analizy ryzyka jest jego pomiar, polegający na określeniu prawdopodobieństwa wystąpienia danego rodzaju ryzyka oraz jego następstw / wpływu.
5. Ocena zarówno prawdopodobieństwa, jak i następstw polega na nadaniu im wartości szacunkowych w przyjętych skalach jakościowo-ilościowych.
6. W analizie ryzyka uwzględnia się częstotliwość wystąpienia ryzyka (liczbę możliwych powtórzeń), jako jeden ze wskaźników prawdopodobieństwa wystąpienia ryzyka.

7. Na podstawie oszacowanego prawdopodobieństwa oraz następstw określa się współczynnik istotności każdego zidentyfikowanego rodzaju ryzyka - poziom istotności, który pokazuje się jako iloczyn prawdopodobieństwa i następstw ryzyka.
8. Określenie współczynnika istotności ryzyka umożliwia dokonanie oceny istotności ryzyka i pozwala na uporządkowanie listy zidentyfikowanych i oszacowanych rodzajów ryzyka według kryterium ich znaczenia dla ewentualnych naruszeń praw lub wolności osób fizycznych.
9. Dla poszczególnych rodzajów zidentyfikowanego i oszacowanego ryzyka wskazuje się rozwiązania (w tym obowiązujące przepisy prawa oraz przyjęte w organizacji procedury, instrukcje i faktycznie podejmowane działania), które mają na celu ograniczenie prawdopodobieństwa lub następstw wystąpienia ryzyka.
10. W razie potrzeby wskazuje się propozycje modyfikacji stosowanych w organizacji rozwiązań lub zgłasza się propozycje nowych rozwiązań (mechanizmów i uregulowań wewnętrznych), których zaplanowanie i wdrożenie w organizacji jest konieczne dla ograniczenia ryzyka.

Przykłady zagrożeń, ryzyk, następstw

§ 5.

Rodzaj zagrożenia	**Opis ryzyka/zagrożenia**	**Następstwa/skutki naruszenia praw lub wolności dla osób fizycznych**
Nieautoryzowane działania	Nieautoryzowane użycie urządzeń	dyskryminacja
	Nieuprawnione kopiowanie oprogramowania	kradzież tożsamości lub oszustwo dot. tożsamości
	Użycie fałszywego lub skopiowanego oprogramowania	strata finansowa
	Zniekształcenie danych	naruszenie dobrego imienia
	Nielegalne przetwarzanie danych	naruszenie poufności danych osobowych chronionych tajemnicą zawodową
Naruszenie bezpieczeństwa funkcji	Błąd użytkowania	nieuprawnione odwrócenie pseudonimizacji
	Naruszenie praw	znaczna szkoda gospodarcza lub społeczna
	Fałszowanie praw	pozbawienie osób, których dane dotyczą przysługujących im praw i wolności lub sprawowania kontroli nad swoimi danymi osobowymi
	Odmowa działania	konieczność ponownego dostarczenia dokumentów
	Naruszenie dostępności personelu	utrata historii przetwarzania danych
	Utrata dostaw prądu	
	Awaria urządzenia telekomunikacyjnego	
	Podsłuch	

	Kradzież nośników lub dokumentów	
	Kradzież urządzenia	
	Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników	
	Ujawnienie	
	Dane z niewiarygodnych źródeł	
	Manipulowanie urządzeniem	
	Sfałszowanie oprogramowania	
	Niewłaściwe funkcjonowanie urządzeń	
Awarie techniczne	Przeciążenie systemu informacyjnego	
Zniszczenia fizyczne	Niewłaściwe funkcjonowanie oprogramowania	
	Awaria urządzenia	
	Pożar	
	Zalanie	
	Zanieczyszczenie	
	Poważny wypadek	
	Zniszczenie urządzeń lub nośników	
Zjawiska naturalne	Zjawiska klimatyczne	
	Zjawiska pogodowe	
	Powódź	

Prawdopodobieństwo wystąpienia ryzyka

§ 6.

1. Oceniając prawdopodobieństwo wystąpienia ryzyka, uwzględnia się możliwą częstotliwość wystąpienia zdarzenia (jak często dane zdarzenie może mieć miejsce). W odniesieniu do czynności powtarzalnych (spraw występujących cyklicznie lub wielokrotnie) uwzględnia się liczbę możliwych powtórzeń (ile razy względem ogólnej liczby spraw zdarzenie może mieć miejsce).
2. Jakościową ocenę prawdopodobieństwa wystąpienia ryzyka wyraża się zarówno procentowo, jak również ilościowo (punktowo), poprzez nadanie prawdopodobieństwu - oszacowanemu w sposób jakościowy - wartości w skali od 1 do 5, gdzie:
   1 - oznacza prawdopodobieństwo znikome (0-20%)
   2 - oznacza prawdopodobieństwo niskie (21-40%)
   3 - oznacza prawdopodobieństwo średnie (41-60%)
   4 - oznacza prawdopodobieństwo wysokie (61-80%)
   5 - oznacza prawdopodobieństwo bardzo wysokie (81-100%)

WYTYCZNE DO OCENY PRAWDOPODOBIEŃSTWA WYSTĄPIENIA I NASTĘPSTW RYZYKA

Skala prawdopodobieństwa wystąpienia ryzyka		Skala następstw ryzyka
Prawdopodobieństwo wystąpienia	**Oszacowane ryzyko**	**Następstwa (wpływ) Oszacowane ryzyko**
Tego typu ryzyko do tej pory jeszcze nigdy nie wystąpiło, **lub/i**, Przy realizacji danego procesu / zadania nie współpracuje się z innymi komórkami/jednostkami, **lub/i**, W ostatnich 3 latach obszar/proces nie podlegał zmianom technologicznym, organizacyjnym i kadrowym, **lub/i**, Oceniany obszar/proces uregulowany jest wyłącznie regulacjami wewnętrznymi.	1 znikome	1 nieznaczne
Tego typu ryzyko wystąpiło 1 raz w okresie ostatnich 3 lat. Ryzyko prawdopodobnie nie wystąpi/może wystąpić w zupełnie wyjątkowych sytuacjach, **lub/i**, Przy realizacji danego zadania/procesu współpracuje się z małą (1 lub 2) liczbą komórek/jednostek, **lub/i**, W okresie ostatnich 3 lat obszar/proces podlegał zmianom technologicznym, organizacyjnym i kadrowym w minimalnym stopniu i uznaje się je za wdrożone, **lub/i**, Zadania/proces w małym zakresie objęty regulacjami o charakterze zewnętrznym. Nie podlegały one zmianom.	2 niskie	2 małe
Tego typu ryzyko wystąpiło 2 razy w okresie ostatnich 3 lat, **lub/i**, Przy realizacji danego celu współpracuje się z dużą (co najmniej 3) liczbą komórek/jednostek, **lub/i**, Zadanie/proces podlegał zmianom organizacyjnym, technologicznym i kadrowym które zakończyły się ponad rok temu, **lub/i**, Zadanie/proces objęty w małym stopniu regulacjami zewnętrznymi, które mogły podlegać w ostatnim okresie pewnym zmianom.	3 średnie	3 średnie
Tego typu ryzyko wystąpiło 3 razy w okresie ostatnich 3 lat. Istnieje wysokie prawdopodobieństwo na wystąpienie tego ryzyka, **lub/i**, Zadanie/proces wymaga współpracy z dużą (więcej niż 3) liczbą komórek i jednostek lub/i podmiotami zewnętrznymi, **lub/i**, W ciągu ostatniego roku obszar/proces podlegał zmianom technologicznym, organizacyjnym i kadrowym, z których część może wymagać poprawek i działań dostosowawczych, **lub/i**, Obszar/proces objęty dużą liczbą regulacji prawnych (zewnętrznych i wewnętrznych), które w ostatnim roku podlegały istotnym zmianom.	4 wysokie	4 poważne

Prawdopodobieństwo wystąpienia	Oszacowane ryzyko	Następstwa (wpływ) Oszacowane ryzyko
Tego typu ryzyko wystąpiło więcej niż 3 razy w okresie ostatnich 3 lat. Istnieje bardzo wysokie prawdopodobieństwo na wystąpienie tego ryzyka, **lub/i**, Zadanie/proces wymaga współpracy z bardzo dużą (więcej niż 10) liczbą komórek i jednostek lub/i podmiotami zewnętrznymi, **lub/i**, W ostatnim roku zadanie/proces podlegał istotnym zmianom technologicznym, organizacyjnym i kadrowym albo obszar podlega częstym zmianom tego typu bądź też obszar jest w trakcie zmian, **lub/i**, Obszar/proces objęty dużą liczbą regulacji prawnych (zewnętrznych i wewnętrznych), które w ostatnim roku podlegały istotnym zmianom lub/i, które zmienią się z pewnością w ciągu najbliższego roku.	5 bardzo wysokie	5 katastrofalne

Następstwo (wpływ)

§ 6.

1. Jakościowa ocena następstw ryzyka opiera się na oszacowaniu potencjalnych skutków, jakie zaistnienie danego rodzaju ryzyka (zdarzenia) może mieć na organizacji. Uwzględnia się przy tym w szczególności konsekwencje prawne, finansowe i organizacyjne zaistnienia danego zdarzenia oraz jego wpływ na prawa bądź wolności dla osób fizycznych.
2. Jakościową ocenę możliwych następstw wystąpienia ryzyka można wyrazić ilościowo (punktowo), poprzez nadanie rozmiarom następstw - oszacowanym w sposób jakościowy - wartości w skali od 1 do 5, gdzie:
   1 - oznacza skutek nieznaczny
   2 - oznacza skutek mały
   3 - oznacza skutek średni
   4 - oznacza skutek poważny
   5 - oznacza skutek katastrofalny

Istotność

§ 7.

1. Określenie prawdopodobieństwa (PR) i następstw (N) ryzyka w skalach pięciostopniowych umożliwia ustalenie współczynnika poziomu istotności ryzyka (IR) jako iloczynu (wyrażonych punktowo) prawdopodobieństwa wystąpienia ryzyka oraz następstw:

IR = PR x N

gdzie:

IR - współczynnik istotności ryzyka
PR - prawdopodobieństwo wystąpienia ryzyka
N - potencjalne następstwa wystąpienia ryzyka.

2. Przyjęty wzór dla obliczenia współczynnika istotności ryzyka zakłada, że poziom zagrożenia w każdym wypadku zależy zarówno od prawdopodobieństwa wystąpienia ryzyka, jak i od następstw, a więc że ryzyko bardzo prawdopodobne, ale wywołujące niewielkie skutki, może mieć podobny stopień istotności, jak ryzyko mało prawdopodobne, ale o poważnych przewidywanych skutkach.
3. Z uwagi na pięciostopniową skalę zarówno prawdopodobieństwa, jak i następstw ryzyka współczynnik istotności danego rodzaju ryzyka może przyjąć wartość od 1 do 25.
4. Mapę ryzyka - matrycę punktowej oceny (współczynnika) istotności ryzyka, zawierającą prezentację ryzyka w macierzy "5x5", przedstawia *załącznik nr 2* do niniejszej Procedury.

Reakcja na ryzyko i działania zaradcze

§ 8.

1. Dla każdego zidentyfikowanego i poddanego analizie ryzyka, jego właściciel wskazuje jedną z poniższych reakcji:
   1) **O**graniczanie - podjęcie działań zaradczych, które doprowadzić mają do likwidacji lub ograniczenia ryzyka do akceptowalnego poziomu.
   2) **D**zielenie się - częściowe lub całkowite przeniesienie ryzyka na inny podmiot,

3) **A**kceptacja (tolerowanie) - oznacza, że nie podejmuje się żadnych działań zaradczych, ale rozumie ewentualne skutki zdarzenia i świadomie godzi się na nie (np.: możliwość przeciwdziałania jest ograniczona lub koszt przeciwdziałania przewyższa potencjalne korzyści),
4) **U**nikanie (likwidacja ryzyka) - niepodejmowanie lub zaprzestanie działania narażającego na ryzyko,

2. Decyzja odnośnie reakcji na ryzyko powinna być podejmowana z uwzględnieniem, z jednej strony potencjalnych kosztów, które wiążą się z jego ograniczaniem, z drugiej zaś potencjalnych korzyści, które wynikają z podjęcia ryzyka.

3. Przy wskazaniu reakcji na ryzyko należy uwzględnić określony w niniejszym dokumencie akceptowany poziom ryzyka. W tym celu należy wykorzystać mapę ryzyka. Mapa ryzyka jest graficzną prezentacją wyników oceny ryzyka. Dla każdego z poziomów ryzyka przypisano odpowiednią kolorystykę:
1) poziom niski - **kolor zielony** - akceptowalny poziom ryzyka, zaplanowanie i wdrożenie działań zaradczych zależy od decyzji właściciela ryzyka,
2) poziom średni - **kolor żółty** - akceptowalny poziom ryzyka, konieczność stałego monitorowania poziomu ryzyka,
3) poziom wysoki - **kolor pomarańczowy** - akceptowalny poziom ryzyka, wymóg stałego monitorowania poziomu ryzyka oraz konieczność zaplanowania działań zaradczych do ewentualnego wdrożenia,
4) poziom bardzo wysoki - **kolor czerwony** - nieakceptowalny poziom ryzyka, konieczność wycofania się lub opracowania i wdrożenia Planu działań sprowadzających ryzyko do akceptowanego poziomu w terminie uzgodnionym z Administratorem danych. Właściciel ryzyka zobowiązany jest do monitorowania poziomu ryzyka i skuteczności przyjętych działań. **Realizacja celów/procesów obciążonych ryzykiem bardzo wysokim wymaga akceptacji Administratora danych oraz przeprowadzeniem oceny skutków dla ochrony danych.** Wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony został opublikowany w Komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r pod pozycją 827.

4. Zastosowane techniczne i organizacyjne środki bezpieczeństwa, mechanizmy kontrolne to działania zaradcze, które mają na celu ograniczenie ryzyka do akceptowanego dla organizacji poziomu - zarówno prawdopodobieństwa, jak i następstw jego wystąpienia.

5. Mechanizmy kontrolne powinny prowadzić do zmniejszenia niepewności wyników poprzez wykrycie i skorygowanie niepożądanych rezultatów, unikanie niepożądanych efektów lub ograniczenie ich występowania, a także osiągnięcie spodziewanych rezultatów.

6. Zastosowane techniczne i organizacyjne środki bezpieczeństwa, mechanizmy kontrolne obejmują przyjęte w organizacji procedury, instrukcje, jak i faktycznie realizowane działania.

7. W razie potrzeby wskazuje się planowane w organizacji działania, mające na celu modyfikację istniejących lub wdrożenie nowych techniczne i organizacyjne środków bezpieczeństwa czy mechanizmów kontrolnych koniecznych dla ograniczenia ryzyka.

8. W odniesieniu do każdego rodzaju ryzyka ustalana jest osoba odpowiedzialna za zarządzanie danym ryzykiem - właściciel ryzyka.
Do zadań właścicieli ryzyka należy, w szczególności:
1) identyfikacja i ocena ryzyk związanych z realizacją przypisanych procesów,
2) określenie istniejących zabezpieczeń, zastosowanych środków technicznych i organizacyjnych,
3) określenie następstw naruszeń praw lub wolności dla osób fizycznych,
4) określenie prawdopodobieństwa, następstw wystąpienia i istotności ryzyka w kontekście następstw dla osób fizycznych,
5) określenie reakcji w odniesieniu do poszczególnych ryzyk,

6) określenie następstw dla organizacji,
7) realizacja organizacyjnych i technicznych środków bezpieczeństwa w stosunku do zidentyfikowanych ryzyk.

Rejestry ryzyk

§ 9.

1. Przynajmniej raz na kwartał dokonuje się w organizacji przeglądu rejestru ryzyk związanych z obszarem ochrony danych. Jest to monitoring ryzyka.

2. Monitoring ryzyka obejmuje:
   a) wykonanie przeglądu, w celu określenia czy ryzyko uległo zmianie,
   b) sprawdzenie czy punktowa ocena ryzyka jest wciąż odpowiednia,
   c) zapewnienie skuteczności dotychczasowych zastosowanych mechanizmów kontrolnych, technicznych i organizacyjne środków bezpieczeństwa,
   d) monitorowanie uzgodnionych działań w zakresie zarządzania ryzykiem.

3. Wzór rejestru ryzyka stanowi załącznik nr 1 do niniejszej procedury.

Załącznik nr 1 do Procedury Zarządzania Ryzykiem - szacowanie ryzyka / wzór /

Lp.	**Opis procesu przetwarzania danych osobowych**	**Opis ryzyka/zagrożenia**	**Istniejące zabezpieczenia / Zastosowane organizacyjne i techniczne środki bezpieczeństwa / mechanizmy kontrolne**	**Następstwa/skutki naruszenia praw lub wolności dla osób fizycznych**	**Prawdopodobieństwo wystąpienia** w skali od 1 do 5	**Następstwa (wpływ)** w skali od 1 do 5	**Istotność** (5 x 6)	**Reakcja na ryzyko O - ograniczanie D - dzielenie się A - akceptacja U - unikanie**	**Następstwa/ skutki dla organizacji**	**Organizacyjne i techniczne środki bezpieczeństwa do zastosowania**	**Właściciel ryzyka** - osoba / dział / komórka odpowiedzialna za minimalizację ryzyka
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	Dziennik elektroniczny	Niewłaściwe funkcjonowanie oprogramowania. Naruszenie integralności systemu	Proces uwierzytelniania Zabezpieczenia antywirusowe Kopie bezpieczeństwa	Naruszenie prywatności Utrata tożsamości	3	4	12	O - ograniczenie	Skutki prawne Odpowiedzialność administracyjna i finansowa	Audyt bezpieczeństwa informatycznego	Administrator systemu informatycznego
2	Rekrutacja do Szkoły/Przedszkola	Kradzież lub utrata dokumentów	Gospodarka kluczami. Fizyczne zabezpieczenie pomieszczeń	Naruszenie prywatności Utrata tożsamości	2	5	10	O - ograniczenie	Utrata reputacji, odpowiedzialność prawna, finansowa	Zamykane na klucz niemetalowe szafy	Kierownik administracyjny
3	Upoważnienia do odbioru dzieci ze świetlicy szkolnej	Naruszenie praw (odbiór dziecka przez osobę nieuprawnioną	Upoważnienia do odbioru dzieci	Znaczne szkody społeczne	3	5	15	O - ograniczenie	Odpowiedzialność prawna	Potwierdzanie tożsamości osób upoważnionych	Wychowawcy, osoby odpowiadające za bezpieczeństwo dzieci na świetlicy

Załącznik nr 2 "Mapa ryzyka" / wzór /

NASTĘPSTWA "y" (wpływ)						
	5 katastrofalne 81-100%		**2. rekrutacja**	**3. Odbiór dzieci**		
	4 poważne 61-80%			**1. e-dziennik**		
	3 średnie 41-60%					
	2 małe 21-40%					
	1 nieznaczne 0-20%					
		1 znikome	**2** niskie	**3** średnie	**4** wysokie	**5** bardzo wysokie
		PRAWDOPODOBIEŃSTWO WYSTĄPIENIA "X"				

Załącznik nr 9

Instrukcja postepowania w sytuacji naruszenia ochrony danych osobowych

Spis treści:

1. Istota naruszenia danych osobowych…….....3

2. Postępowanie w przypadku naruszenia danych osobowych ……..……3

3. Naruszenie danych osobowych – odpowiedzialność …….....……5

4. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczem ……..5

5. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych....6

Załącznik nr 1 raport z naruszenia ochrony danych…….....……6
Załącznik nr 2 rejestr incydentów bezpieczeństwa i działań korygujących
i zapobiegawczych… …….7
Załącznik nr 3 zgłoszenie naruszenia ochrony danych osobowych organowi
nadzorczemu ……..8

I. Istota naruszenia danych osobowych

§ 1

Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1. nieautoryzowany dostęp do danych,
2. nieautoryzowane modyfikacje lub zniszczenie danych,
3. udostępnienie danych nieautoryzowanym podmiotom,
4. nielegalne ujawnienie danych,
5. pozyskiwanie danych z nielegalnych źródeł.

II. Postepowanie w przypadku naruszenia danych osobowych

§ 2

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Inspektorowi ochrony danych.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych:
   - 2.1. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
   - 2.2. dokumentacja jest niszczona bez użycia niszczarki;
   - 2.3. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
   - 2.4. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.
   - 2.5. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,
   - 2.6. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
   - 2.7. wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;
   - 2.8. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
   - 2.9. stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
   - 2.10. telefoniczne próby wyłudzenia danych osobowych;
   - 2.11. kradzież komputerów lub twardych dysków z danymi osobowymi;
   - 2.12. utrata kontroli nad kopią danych osobowych;
   - 2.13. maile zachęcające do ujawnienia identyfikatora i/lub hasła;

2.14. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
2.15. istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki"
2.16. hasła do systemów przechowywane są w pobliżu komputera.

§ 3

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .

§ 4

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osoby upoważnionej przez Administratora danych.

§ 5

Administrator Systemu Informatycznego lub upoważniona osoba jest zobowiązana do informowania Administratora o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6

Administrator podejmuje następujące kroki:

1. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
2. odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
3. nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7

Administrator lub osoba upoważniona dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - Załącznik nr 1.

§ 8

Administrator lub osoba upoważniona zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) - Załącznik nr 2 - rejestr incydentów i działań korygujących i zapobiegawczych

III. Naruszenie danych osobowych - odpowiedzialność

§ 9

Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

IV. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczmu

§ 10

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 Urzędowi ochrony danych, 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. Wzór zgłoszenia – Załącznik nr 3.
2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
   2.1. 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;
   2.2. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   2.3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   2.4. opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – 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 musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

V. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

§ 11

1. 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.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 lit. b), c) i d).
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   3.1. 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;
   3.2. 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.

Załącznik nr 1

RAPORT Z NARUSZENIA OCHRONY DANYCH

1. Data ..... Godzina .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem

   .....
   (imię, nazwisko, stanowisko służbowe,):

3. Lokalizacja zdarzenia
   ..... (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

   .....

5. Podjęte działania:

   .....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

   .....

7. Postępowanie wyjaśniające i naprawcze:

   .....

..... (podpis pracownika)

..... (data i podpis Inspektora ochrony danych)

Załącznik nr 2

REJESTR INCYDENTÓW BEZPIECZEŃSTWA ORAZ DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH

Zadanie / problem / incydent (*podać opis incydentu*)	Źródło zgłoszenia (*podać źródło zgłoszenia np. zawiadomienie, kontrola, itd.*)	Data rozpoczęcia	Data zakończenia	Odpowiedzialny za realizację (*podać dane osoby lub funkcje osoby odpowiedzialnej*)	Przyczyna niezgodności (*podać przyczynę powstania incydentu*)	Działanie korygujące / zapobiegawcze (*opisać działania jakie podjęto w celu przywrócenia bezpieczeństwa*)	Ocena skuteczności (*opisać jakie skutki przyniosło działanie korygujące*)

Załącznik nr 3

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

W jaki sposób powiadomić Prezesa UODO o naruszeniu?

Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

1. Zgłoszenia naruszenia dokonuje się elektronicznie **za pomocą odpowiedniego formularza dostępnego poniżej**,
   https://uodo.gov.pl/pl/134/233

   który należy wypełnić a następnie...

2. ...załączyć do **pisma ogólnego dostępnego na platformie biznes.gov.pl**

Załącznik nr 10

Umowa

powierzenia przetwarzania danych osobowych

stanowiąca uzupełnienie Umowy .....

zawarta w dniu ..... w ....., pomiędzy:

..... („**Administrator**”)

a

..... („**Przetwarzający**”)

(dalej łącznie jako: „**Strony**”)

Mając na uwadze, że:

i. Strony zawarły umowę ..... („**Umowa Podstawowa**”), w związku, z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym Umową;

ii. Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania Danych Osobowych w imieniu Administratora;

iii. Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania Danych Osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO**.

Strony postanowiły zawrzeć Umowę o następującej treści:

przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora

1. Opis Przetwarzania

1.1. **Przedmiot [art. 28 ust. 3 RODO**] Na warunkach określonych niniejszą Umową oraz Umową Podstawową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych Danych Osobowych.

1.2. **Czas [art. 28 ust. 3 RODO**] Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.

1.3. **Charakter i cel [art. 28 ust. 3 RODO**] Charakter i cel przetwarzania wynikają z Umowy Podstawowej. W szczególności:

1.3.1. charakter przetwarzania określony jest następującą rolą Przetwarzającego [*przykład: obsługa księgowa Administratora*], zaś

1.3.2. celem przetwarzania jest [*przykład: umożliwienie Administratorowi wywiązywania się z prawnych obowiązków związanych z prowadzeniem rachunkowości, a także w celu zarządzania finansowego Administratora*]

1.4. **Rodzaj danych [art. 28 ust. 3 RODO**] Przetwarzanie obejmować będzie następujące rodzaje danych osobowych („**Dane**”):

Dane zwykłe:

(1) imię i nazwisko,

(2) numer ewidencyjny PESEL,

(3) adres e-mail,

(4) adres IP,

(5) numery telefonów,

(6) adres zamieszkania,

(7) data urodzenia,

(8) NIP,

(9) seria i numer dokumentu tożsamości,

(10) imiona rodziców,

(11) numer rachunku bankowego,

(12) .....

Dane szczególnych kategorii i dane karne:

(13) dokumentacja medyczna,

(14) .....,

(15) .....

Dane dzieci

(16) imię i nazwisko,

(17) data urodzenia,

(18) adres e-mail,

(19) pseudonim,

(20) .....

Dane nieustrukturyzowane

(21) kontent o potencjalnej i prawdopodobnej zawartości danych osobowych (wpisy, dokumenty tekstowe, obrazy, nagrania, filmy).

1.5. **Kategorie osób [art. 28 ust. 3 RODO**] Przetwarzanie Danych będzie dotyczyć następujących kategorii osób:

(1) pracownicy Administratora i podmiotów stowarzyszonych Administratora,

(2) klienci usługi/produktu Administratora określonych w Umowie Podstawowej,

(3) osoby, z którymi klienci Administratora wchodzą w interakcje społeczne,

(4) kontrahenci (odbiorcy i dostawcy) klientów administratora,

(5) odbiorcy korespondencji elektronicznej klientów Administratora,

(6) .....,

(7) .....,

(8) .....,

2. Podpowierzenie

2.1. **Podpowierzenie [art. 28 ust. 2 RODO**] Przetwarzający może powierzyć konkretne operacje przetwarzania Danych („**podpowierzenie**”) w drodze pisemnej umowy podpowierzenia („**Umowa Podpowierzenia**”) innym podmiotom przetwarzającym. („**Podprzetwarzający**”), pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora lub braku sprzeciwu.

2.2. **Zaakceptowani Podprzetwarzający.** Lista Podprzetwarzających zaakceptowanych przez Administratora stanowi **Załącznik nr 1 do Umowy – Lista Zaakceptowanych Podprzetwarzających**.

2.3. **Sprzeciw.** Powierzenie przetwarzania Danych Podprzetwarzającym spoza Listy Zaakceptowanych Podprzetwarzających wymaga uprzedniego zgłoszenia Administratorowi w celu umożliwienia wyrażenia sprzeciwu. Administrator może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia Danych konkretnemu Podprzetwarzającemu. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć Danych Podprzetwarzającemu objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego Podprzetwarzającego, musi niezwłocznie zakończyć podpowierzenie temu Podprzetwarzającemu. Wątpliwości co do zasadności sprzeciwu i ewentualnych negatywnych konsekwencji Przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.

2.4. **Transfer obowiązków [art. 28 ust. 4 RODO**] Dokonując podpowierzenia Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków

Przetwarzającego wynikających z niniejszej Umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.

2.5. **Zobowiązanie względem Administratora.** Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia, zawierającego listę obowiązków Podprzetwarzającego.

2.6. **Zakaz podzlecenia świadczenia głównego [art. 28 ust. 4 RODO**] Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy.

3. Obowiązki Przetwarzającego

Przetwarzający ma następujące obowiązki:

3.1. **Udokumentowane polecenia [art. 28 ust. 3 lit. a RODO]** Przetwarzający przetwarza Dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.

3.2. **Nieprzetwarzanie poza EOG [art. 28 ust. 3 lit. a RODO]** Przetwarzający oświadcza, że nie przekazuje Danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy („**EOG**”)). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.

3.3. **Poinformowanie o zamiarze przetwarzania poza EOG. [art. 28 ust. 3 lit. a RODO]** Jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać Dane poza EOG, informuje o tym Administratora, w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.

3.4. **Tajemnica [art. 28 ust. 3 lit. b RODO]** Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania Danych w wykonaniu Umowy, udokumentowane zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.

3.5. **Bezpieczeństwo [art. 28 ust. 3 lit. c RODO]** Przetwarzający zapewnia ochronę Danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy.

3.6. **Podprzetwarzanie [art. 28 ust. 3 lit. d RODO]** Przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (Podprzetwarzającego).

3.7. **Współpraca przy realizacji praw jednostki [art. 28 ust. 3 lit. e RODO]** Przetwarzający zobowiązuje się wobec Administratora do odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO („**Prawa jednostki”**). Przetwarzający oświadcza, że zapewnia obsługę Praw jednostki w odniesieniu do powierzonych Danych. Szczegóły obsługi Praw jednostki zostaną pomiędzy Stronami uzgodnione. Strony ustaliły procedurę obsługi Praw jednostki odrębnym dokumentem.

3.8. **Wsparcie przy obowiązkach bezpieczeństwa [art. 28 ust. 3 lit. f RODO]** Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora obowiązków z

obszaru ochrony danych osobowych, o których mowa w art. 32−36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).

3.9. **Legalność poleceń [art. 28 ust. 3 ak. 2 RODO]** Jeżeli Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.

3.10. **Projektowanie prywatności [art. 25 ust. 1 RODO**] Planując dokonanie zmian w sposobie przetwarzania Danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa Danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania Danych przez Przetwarzającego.

3.11. **Minimalizacja [art. 25 ust. 2 RODO**] Przetwarzający zobowiązuje się do ograniczenia dostępu do Danych Osobowych wyłącznie do osób, których dostęp do Danych jest potrzebny dla realizacji Umowy i posiadających odpowiednie upoważnienie.

3.12. **RCPD [art. 30 ust. 2 RODO]** Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania Danych, w tym rejestru czynności przetwarzania danych osobowych (wymóg art. 30 RODO). Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.

3.13. **Profilowanie [art. 13 i 14 RODO**] Jeżeli Przetwarzający wykorzystuje w celu realizacji Umowy zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.

3.14. **Szkolenie personelu** Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania Danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

4. Obowiązki Administratora

4.1. Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

5. Bezpieczeństwo danych

5.1. **Bezpieczeństwo danych osobowych [art. 32 RODO**] Przetwarzający przeprowadził analizę ryzyka przetwarzania powierzonych Danych, udostępnił ją Administratorowi i stosuje się do jej wyników, co do organizacyjnych i technicznych środków ochrony danych.

5.2. **Środki bezpieczeństwa.** Strony uzgodniły odrębnym dokumentem poziom zabezpieczeń Danych wymagany po stronie Przetwarzającego.

5.3. **Gwarancje bezpieczeństwa.** Przetwarzający przedstawił Administratorowi informacje i dokumenty potwierdzające, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Obie Strony zachowują kopie przedstawionych dokumentów i dowody przedstawienia informacji, dla potrzeb spełnienia wymogu rozliczalności.

6. Powiadomienie o Naruszeniach Danych Osobowych

6.1. **Powiadomienie o naruszeniu.** Przetwarzający powiadamia Administratora danych o każdym podejrzeniu naruszenia ochrony Danych osobowych nie później niż w 24 godziny od pierwszego zgłoszenia, umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.

6.2. **Rozwinięcie.** Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru.

7. Nadzór

7.1. **Sprawowanie kontroli [art. 28 ust. 3 lit. h RODO**] Administrator kontroluje sposób przetwarzania powierzonych Danych Osobowych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do (i) wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe oraz (ii) wglądu do dokumentacji związanej z przetwarzaniem Danych Osobowych. Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania Danych Osobowych, oraz udostępnienia rejestrów przetwarzania.

7.2. **Współpraca przy kontroli. [art. 28 ust. 3 lit. h RODO**] Przetwarzający współpracuje z urzędem ochrony danych osobowych w zakresie wykonywanych przez niego zadań.

7.3. Przetwarzający:

(1) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO,

(2) umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzanie audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.

8. Oświadczenia Stron

8.1. **Oświadczenie Administratora**. Administrator oświadcza, że jest Administratorem Danych oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.

8.2. **Oświadczenie Przetwarzającego [art. 28 ust. 1 RODO**]**.** Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem

danych osobowych objętym Umowa i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.

8.3. **Referencje [art. 28 ust. 1 RODO].** Na żądanie Administratora Przetwarzający okaże Administratorowi stosowne referencje, wykaz doświadczenia, informacje finansowe lub inne dowody, iż Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

9. Odpowiedzialność

9.1. **Odpowiedzialność Przetwarzającego [art. 82 ust. 3 RODO**] Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub nie zastosowaniem właściwych środków bezpieczeństwa.

9.2. **Odpowiedzialność za Podprzetwarzających [art. 28 ust. 4 RODO**] Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.

10. Okres Obowiązywania Umowy Powierzenia [art. 28 ust. 3 RODO]

10.1. Umowa została zawarta na czas obowiązywania Umowy Podstawowej.

11. Usunięcie Danych

11.1. **Usunięcie danych [art. 28 ust. 3 lit g RODO]** Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych Danych i jest zobowiązany do:

(1) usunięcia Danych,

(2) usunięcia wszelkich ich istniejących kopii lub zwrotu Danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie Danych.

(3) Strony uzgodnią sposób usunięcia Danych odrębnym dokumentem w ciągu 30 dni od zawarcia Umowy Powierzenia.

11.2. **Karencja**. Przetwarzający dokona usunięcia Danych po upływie 180 dni od zakończenia Umowy, chyba że Administrator poleci mu to uczynić wcześniej.

11.3. **Oświadczenie**. Po wykonaniu zobowiązania, o którym mowa w pkt 10.1., Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich Danych.

12. Postanowienia Końcowe

12.1. **Pierwszeństwo.** W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy Powierzenia a Umowy Podstawowej, pierwszeństwo mają postanowienia Umowy Powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.

12.2. **Egzemplarze**. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

12.3. **Właściwość prawa.** Umowa podlega prawu polskiemu oraz RODO.

Załącznik nr 11

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych

I. Cele wprowadzenia i zakres stosowania Instrukcji Zarządzania Systemem Informatycznym.

1. „Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Szkole Podstawowej nr 2 w Woli Rzędzińskiej ", zwana dalej instrukcją, została wprowadzona w celu spełnienia wymagań, o których jest mowa w art. 24 ust. 1 i ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych lub RODO) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych (Dz. U. 2004 r., nr 100, poz. 1024), tj. zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Instrukcja jest dokumentem powiązanym z „Polityką bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Szkole Podstawowej nr 2 w Woli Rzędzińskiej" i wraz z nim składa się na dokumentację wymaganą przez art. 36. ust. 2. ustawy o ochronie danych osobowych.

3. Niniejsza instrukcja znajduje zastosowanie do systemów informatycznych, stosowanych w SP nr 2 w Woli Rzędzińskiej, w których są przetwarzane dane osobowe.

4. Instrukcja podlega monitorowaniu i w razie potrzeby uaktualnianiu co roku, do końca stycznia, przez administratora danych osobowych lub upoważnioną przez niego osobę, w ramach sprawowania kontroli zarządczej.

5. Dokument instrukcji przechowywany jest w wersji papierowej i elektronicznej.

II. DEFINICJE.

Ilekroć w instrukcji jest mowa o:

1) **administratorze danych osobowych** – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych. W Szkole Podstawowej nr 2 w Woli Rzędzińskiej funkcję administratora danych pełni dyrektor szkoły;

administratorze systemu – rozumie się przez to osobę nadzorującą pracę systemu informatycznego oraz wykonującą w nim czynności wymagane specjalnych uprawnień;

dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów;

przetwarzanie danych – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywania, udostępnianie, zmienianie, usuwanie;

haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to pracownika szkoły, która upoważniona została do przetwarzania danych osobowych przez dyrektora szkoły na piśmie;

poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;

raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

rozporządzeniu MSWiA – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych (Dz.U. z 2004 r., nr 100, poz. 1024.);

serwisancie – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;

sieci publicznej – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;

systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

ustawie – ustawę z 10.05.2018 r. o ochronie danych osobowych (Dz.U. poz. 1000 ze zm.);

uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

użytkowniku – rozumie się przez to pracownika szkoły upoważnionego do przetwarzania danych osobowych, zgodnie z zakresem obowiązków, któremu nadano identyfikator i przyznano hasło.

III. NADAWANIE I REJESTROWANIE (WYREJESTROWANIE) UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM.

1. Nadawanie i rejestrowanie uprawnień.

1) Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez dyrektora szkoły lub uprawnioną przez niego osobę.

2) Rejestracja użytkownika, o którym jest mowa w pkt. 1., polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

2. Wyrejestrowanie uprawnień.

1) Wyrejestrowanie użytkownika systemu informatycznego dokonuje dyrektor szkoły lub upoważniona przez niego osoba.

2) Wyrejestrowanie, o którym jest mowa w pkt. 1., może mieć charakter czasowy lub trwały.

3) Wyrejestrowanie następuje przez:
a) zablokowanie konta użytkownika do czasu ustania przyczyny, uzasadniającej blokadę (wyrejestrowanie czasowe),
b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4) Czasowe wyrejestrowanie użytkownika z systemu musi nastąpić w razie:
a) nieobecności użytkownika w pracy, trwającej dłużej niż 21 dni kalendarzowych,
b) zawieszenia w pełnieniu obowiązków służbowych.

5) Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
a) wypowiedzenie umowy o pracę,
b) wszczęcie postępowania dyscyplinarnego.

6) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

IV. METODY I ŚRODKI UWIERZYTELNIENIA.

1. Każdy użytkownik systemu informatycznego otrzymuje od administratora bezpieczeństwa informacji identyfikator i hasło.

2. Identyfikator składa się z sześciu znaków, z których dwa pierwsze odpowiadają dwóm pierwszym literom imienia użytkownika, a cztery kolejne- czterem pierwszym literom jego nazwiska. W identyfikatorze pomija się polskie znaki diakrytyczne./ wpisać własne/

3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika systemu administrator bezpieczeństwa informacji nadaje inny identyfikator, odstępując od zasady określonej w pkt. 1.

4. Hasło użytkownika powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

5. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

6. Zmiana haseł w systemie następuje nie rzadziej niż co 30 dni.

V. PROCEDURY ZWIĄZANE Z GROMADZENIEM, PRZECHOWYWANIEM, PRZETWARZANIEM, USUWANIEM DANYCH OSOBOWYCH.

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informacyjnym oraz wskazanie osoby odpowiedzialnej za te czynności.

1) Przetwarzać dane osobowe w systemie informatycznym może wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych (wzór tego upoważnienia stanowi załącznik do zarządzenia dyrektora szkoły). Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego, przetwarzającego dane osobowe, następuje na wniosek dyrektora szkoły.

2) Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia upoważnienia zostaje dołączona do akt osobowych pracownika.

3) Identyfikator i hasło do systemu informatycznego, przetwarzającego dane osobowe, są przydzielone użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada

administrator bezpieczeństwa informatycznego. Wyrejestrowanie użytkownika z systemu informatycznego następuje na wniosek administratora danych osobowych.

4) Administrator jest zobowiązany do przeprowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych w Szkole Podstawowej nr 2 w Woli Rzędzińskiej.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2) Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiada za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje.

3) Identyfikator i hasło użytkownika powinny odpowiadać wymaganiom, określonym w rozdziale IV.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1) Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy, mogące świadczyć o naruszeniu ochrony danych osobowych.

2) Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

3) Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z administratorem bezpieczeństwa informacji. Użytkownik informuje administratora bezpieczeństwa informacji o zablokowaniu dostępu do zbioru danych.

4) W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut automatycznie włączony jest wygaszasz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu.

5) Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólne konto użytkownika.

6) W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut, użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje, oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki informacji, zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

7) Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych, służących do ich przetwarzania.

1) Dane osobowe, przetwarzane w systemie informatycznym, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada administrator systemu informatycznego lub osoba specjalnie w tym celu wyznaczona.

2) Kopie zapasowe informacji przechowywanych w systemie informatycznym, przetwarzającym dane osobowe, tworzone są w następujący sposób:

a) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest po wprowadzeniu zmian do aplikacji, kopie umieszczone są na nośnikach wymiennych, kopia przechowywana jest w zamkniętej szafie,
b) kopia zapasowa danych osobowych przetwarzanych przez aplikację (pełna kopia) wykonywana jest codziennie na dysku komputera wybranego przez administratora systemu informatycznego,
c) zbiorcze (tygodniowe) kopie przechowywane są przez okres dwóch tygodni, po tym terminie stare kopie są niszczone poprzez nadpisywanie ich przez bardziej aktualne.

3) W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego, przetwarzającego dane osobowe, których to dotyczy, muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje administrator systemu informatycznego lub osoba przez niego upoważniona.

4) Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych danych.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

1) Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.

2) Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza budynek szkoły powinno odbywać się za wiedzą administratora bezpieczeństwa informacji.

3) W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie ze wskazówkami umieszczonymi w punkcie 4. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

4) W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona znajduje.

6. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1) W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu, konieczne jest podjęcie odpowiednich środków ochronnych.

2) Można wyróżnić następujące rodzaje występujących tu zagrożeń:

- nieuprawniony dostęp bezpośrednio do bazy danych,
- uszkodzenie kodu aplikacji, umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
- przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci internet,
- przechwycenie danych z aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
- uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy, zakłócający pracę aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

3) W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:

- autoryzację użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
- stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
- stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

4) Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje, pochodzące z nośników wymiennych, uruchamiane i odczytywane na stacji roboczej.

5) W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego, przetwarzający dane osobowe, lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialny za zarządzanie systemem, wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

- rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
- antywirusowy skaner ruchu internetowego powinien być stale włączony,
- monitor, zapewniający ochronę przed wirusami w dokumentach MS Office, powinien być stale włączony,
- skaner poczty elektronicznej powinien być stale włączony.

6) Systemy antywirusowe, zainstalowane na stacjach roboczych, powinny być skonfigurowane w sposób następujący:

- zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
- możliwość centralnego uaktualnienia wzorców wirusów.

7) System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

8) Użytkownicy systemu informatycznego zobowiązani są do następujących działań:

- skanowania zawartości dysków stacji roboczej, pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przynajmniej 2 razy w tygodniu,

- skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej, pracującej w systemie informatycznym, pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
- skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

9) W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania, zmierzające do usunięcia zagrożenia.

W szczególności działania te mogą obejmować:

- usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
- odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
- samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

10) System informatyczny, przetwarzający dane osobowe, powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w co najmniej:

- filtry zabezpieczające stacje robocze przed skutkami przepięcia,

7. Sposób realizacji wymogów, o których mowa w § 7 ust. 1. pkt. 4. rozporządzenia MSWiA.

1) System informatyczny, przetwarzający dane osobowe, musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy, pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

2) System informatyczny, przetwarzający dane osobowe, musi posiadać mechanizmy, pozwalające na odnotowanie faktu wykonania operacji na danych.
W szczególności zapis ten powinien obejmować:

- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom niebędącym właścicielem ani współwłaścicielem systemu,
- nieudane próby dostępu do systemu informatycznego, przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,

- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

3) Zapis działań użytkownika uwzględnia:
- identyfikator użytkownika,
- datę i czas, w którym zdarzenie miało miejsce,
- rodzaj zdarzenia,
- określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

4) Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:
- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,
- sposobu przekazania danych.

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

1) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego, przetwarzającego dane osobowe, muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

2) Prace serwisowe na terenie szkoły, prowadzone w tym zakresie, mogą być wykonywane wyłącznie przez jego pracowników lub przez upoważnionych przedstawicieli wykonawców zewnętrznych, znajdujących się w towarzystwie pracowników.

3) Przed rozpoczęciem prac serwisowych przez osoby spoza szkoły konieczne jest potwierdzenie tożsamości serwisantów.

4) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

VI. POZIOM BEZPIECZEŃSTWA

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym, połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu § 6. rozporządzenia.

VII. STOSOWANE ŚRODKI BEZPIECZEŃSTWA

1. Zgodnie z treścią § 6. ust. 4 rozporządzenia o którym jest mowa w pkt. 1.1. niniejszej instrukcji stosuje się w szkole środki bezpieczeństwa na poziomie wysokim.

2. W szkole stosuje się następujące środki bezpieczeństwa:

1) Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2) Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

3) Stosowane są mechanizmy kontroli dostępu do danych.

4) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.

5) W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.

6) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów, służących do przetwarzania danych osobowych.

7) Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności.

8) Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

9) 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 osoby upoważnionej przez administratora danych.

10) W przypadku, gdy do uwierzytelnienia użytkowników używa się haseł, hasło to składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.

11) Urządzenia i nośniki, zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

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

VIII. POSTANOWIENIA KOŃCOWE.

1. Osobą odpowiedzialną za przegląd przestrzegania instrukcji, przegląd jej aktualności oraz aktualizację, a także nadawanie praw dostępu do systemu informatycznego jest administrator bezpieczeństwa informacji lub inna osoba upoważniona przez administratora danych.

2. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie (***załącznik nr 5***), potwierdzające znajomość jej treści.

4. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52. kodeksu pracy.

Załącznik nr 12

Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko upoważnionej osoby	Data udzielenia upoważnienia	Data ustania upoważnienia	Zakres upoważnienia - kategorie danych lub rodzaj czynności lub operacji	Wyłączenia kategorii danych lub czynności, które wynikają z upoważnienia	Identyfikator nadany do przetwarzania w systemie informaty-cznym
1.						
2.						
3.						

Załącznik nr 14

Regulamin funkcjonowania Inspektora Ochrony Danych

1. Wyznaczenie inspektora ochrony danych

1. Szkole Podstawowej nr 2 w Woli Rzędzińskiej jako Administrator, na podstawie Art. 37 ust. 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO), oraz na podstawie art. 9 ustawy z dnia 10.05.2018 r. o ochronie danych osobowych, wyznaczył Inspektora ochrony danych (dalej również IOD).
2. Szczegóły wyznaczenia IOD opisuje załącznik nr 1 do niniejszego Regulaminu.

2. Zadania Inspektora ochrony danych

1. Inspektor ochrony danych ma następujące zadania:
   1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia - RODO, oraz innych przepisów Unii lub krajowych o ochronie danych i doradzanie im w tej sprawie;
   2) monitorowanie przestrzegania rozporządzenia-RODO, innych przepisów Unii lub krajowych o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
   4) współpraca z organem nadzorczym;
   5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
3. Inspektor ochrony danych wypełnia swoje zadania z uwzględnieniem wytycznych dotyczących inspektorów ochrony danych przyjętych przez Grupę Roboczą Art. 29 ds. Ochrony Danych.
4. IOD wypełnia swoje zadania z należytą starannością i w zgodzie z etyką zawodową, ze szczególnym uwzględnieniem KODEKSU ETYKI INSPEKTORA OCHRONY DANYCH przyjętego przez Stowarzyszenie Inspektorów Ochrony Danych SABI.
5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań - zgodnie z prawem Unii i prawem krajowym.

3. Status inspektora ochrony danych

1. Administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
2. Administrator wspiera Inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania

3. Administrator zapewnia, by Inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Inspektor ochrony danych bezpośrednio podlega Dyrektorowi Szkoły.
4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia - RODO.
5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań - zgodnie z prawem krajowym.
6. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

4. Odwołanie lub zmiana Inspektora ochrony danych

1. Inspektor ochrony danych nie jest odwoływany ani karany przez administratora za należyte wypełnianie swoich zadań. IOD nie może zostać odwołany ani karany za udzielenie określonego zalecenia dotyczącego bezpieczeństwa danych osobowych, z którym nie zgadza się Administrator.
2. Zgodnie z regułami, przepisami karnymi i prawa pracy, jak w przypadku każdego innego pracownika czy zleceniobiorcy, Inspektor Ochrony Danych może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie obowiązków IOD (np. kradzież, nękanie fizyczne i psychiczne, molestowanie seksualne, ciężkie naruszenie obowiązków).
3. Administrator zawiadamia Prezesa Urzędu o każdej zmianie danych IOD oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.

5. Dane kontaktowe Inspektora ochrony danych

1. Administrator udostępnia dane inspektora, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej.
2. Administrator zaleca poinformowanie pracowników o imieniu, nazwisku i danych kontaktowych Inspektora ochrony danych.
3. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia - RODO.
4. Kontaktowy adres e-mail Inspektora ochrony danych to ***firma.tomaszpilch@onet.pl***

6. Zespół Inspektora ochrony danych.

1. IOD powinien mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą i współpracy z właściwym organem nadzorczym przy pomocy zespołu.
2. Skład, struktura, podział i zakres obowiązków zespołu IOD może zostać określony w terminie późniejszym i odwołany w każdym czasie.

Załącznik nr 14

ZASADY REALIZACJI PRAW OSÓB, WYNIKAJĄCE Z RODO

1. Każdej osobie, której dane osobowe są przetwarzane przysługują prawa określone w art. 15-22 RODO, w tym:

a. prawo dostępu do danych jej dotyczących
b. prawo do sprostowania danych
c. prawo do usunięcia danych
d. prawo do ograniczenia przetwarzania
e. prawo do przenoszenia danych
f. prawo do sprzeciwu na przetwarzanie jej danych
g. prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu
h. prawo do uzyskania kopii danych

2. Rozpatrywanie żądań osoby, której dane dotyczą odbywa się po zweryfikowaniu tożsamości tej osoby.

3. Jeżeli istnieją uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15-21, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

4. Jeżeli nie można jednoznacznie potwierdzić tożsamości wnoszącego żądanie, odmawia się realizacji żądania.

5. W sytuacji powierzania danych podmiotom przetwarzającym lub udostępniania danych innym administratorom danych należy ich powiadamiać o każdym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, które było wynikiem realizacji wniosku otrzymanego od osoby, której dane dotyczą.

6. Na wnioski dotyczące żądań realizacji praw osób należy udzielać odpowiedzi niezwłocznie, w terminie nie przekraczającym miesiąca od otrzymania żądania.

7. W razie potrzeby termin udzielenia odpowiedzi można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W takim wypadku w terminie miesiąca od otrzymania żądania należy poinformować osobę, której dane dotyczą o przedłużeniu terminu, z podaniem przyczyn opóźnienia.

8. Jeśli żądanie zostało przekazane elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

9. W przypadku nie podjęcia działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje się osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do Prezesa UODO oraz skorzystania ze środków ochrony prawnej przed sądem.

10. Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, można:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
b) odmówić podjęcia działań w związku z żądaniem.

11. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

12. Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 13 i 14, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego.

13. W imieniu małoletniego wniosek składa jego rodzic lub opiekun prawny.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. Sekretarz szkoły– w zakresie realizacji wniosku kierowanego do szkoły.
2. Inspektor ochrony danych [IOD] w zakresie konsultowania sposobu realizacji wniosku.

POSTANOWIENIA OGÓLNE PROCEDURY

1. Sekretarz szkoły jest odpowiedzialny za przyjmowanie, rejestrowanie wniosków.
2. Korespondencję pisemną lub przesłaną elektronicznie za pośrednictwem poczty e-mail lub poprzez system e-PUAP, której treść wskazuje na wniosek obywatela w zakresie praw związanych z ochroną danych osobowych, należy niezwłocznie przekazać do IOD.
3. IOD weryfikuje tożsamość wnioskodawcy oraz czy informacje podane we wniosku umożliwiają udzielenie odpowiedzi na przesłany wniosek. Jeżeli nie zostało to zrealizowane wcześniej, sekretarz szkoły przekazuje wnioskodawcy klauzulę informacyjną dotyczącą przetwarzania na potrzeby realizacji praw osoby, której dane dotyczą.
4. W przypadku braku możliwości potwierdzenia tożsamości, IOD wzywa wnioskodawcę do podania informacji, które umożliwią weryfikację tożsamości. Brak odpowiedzi lub uznanie, że dodatkowe informacje są niewystarczające, skutkuje przekazaniem wnioskodawcy informacji o odmowie zrealizowania wniosku. W takim wypadku należy wskazać sposób ponownego złożenia wniosku.
5. Po skutecznym zweryfikowaniu tożsamości wnioskodawcy, IOD przekazuje treść wniosku do sekretarza szkoły w celu uzyskania informacji o możliwości zrealizowania wniosku.
6. Sekretarz szkoły niezwłocznie weryfikuje możliwość zrealizowania wniosku i przekazuje do IOD informacje o działaniach, które zostały zrealizowane w związku z otrzymanym wnioskiem.
7. W przypadku, gdy korespondencja, której treść wskazuje na wniosek obywatela w zakresie przysługujących mu praw wynikających z przepisów RODO, została przesłana bezpośrednio do szkoły, odbiorca korespondencji zobowiązany do niezwłocznego przekazania wniosku do IOD.
8. IOD odnotowuje informację o sposobie załatwienia sprawy.

Rozdział II. Prawo do sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
2. Ponadto osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
3. Pracownik merytoryczny, który w ramach wykonywanych zadań przetwarza dane osoby wnioskującej i otrzymał od IOD wniosek o sprostowanie danych, obowiązany jest dokonać weryfikacji przetwarzanych danych. Uzupełnienie danych następuje z uwzględnieniem celów przetwarzania.
4. Prawo do sprostowania danych nie znajduje zastosowania do danych osobowych, w odniesieniu do których tryb ich sprostowania lub uzupełnienia określają odrębne przepisy, np. procedura sprostowania błędów i omyłek zawartych w decyzji administracyjnej w trybie art. 113 Kodeksu postępowania administracyjnego.

Rozdział III. Prawo do żądania usunięcia danych

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych. Należy bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
3) dane osobowe były przetwarzane niezgodnie z prawem;
4) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega administrator.

2. Jeżeli dane osobowe zostały upublicznione, a na mocy ust. 1 istnieje obowiązek usunięcia tych danych osobowych, to (biorąc pod uwagę dostępną technologię i koszt realizacji) podejmuje się niezbędne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, że obywatel, którego dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3. Przepisy ust. 1 i 2 nie mają zastosowania w zakresie, w jakim przetwarzanie jest niezbędne:

1) do korzystania z prawa do wolności wypowiedzi i informacji lub
2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega administrator lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, lub
3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania, lub
4) do ustalenia, dochodzenia lub obrony roszczeń.

Rozdział IV. Prawo do żądania ograniczenia przetwarzania

1. Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania jej danych osobowych.

2. Ograniczenie przetwarzania oznacza, że dane osobowe można jedynie przechowywać. Inne formy przetwarzania mogą mieć miejsce wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

3. Do ograniczenia może dojść w następujących przypadkach:

1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych; w tym przypadku ogranicza się przetwarzanie na okres pozwalający sprawdzić prawidłowość danych;
2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
4) osoba, której dane dotyczą, wobec przetwarzania wniósł sprzeciw. W tym przypadku ogranicza się przetwarzanie do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu.

4. Ograniczenia przetwarzania dokonuje się poprzez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej, tak aby każdy pracownik administratora, który jest upoważniony do przetwarzania tych danych był świadomy, że dane te można jedynie przechowywać.

5. Przed uchyleniem ograniczenia przetwarzania informuje się o tym osobę, która żądała ograniczenia.

Rozdział V. Prawo do przeniesienia danych

1. Jeżeli przetwarzanie odbywa się na podstawie umowy, której stroną jest osoba, której dane dotyczą, oraz w sposób zautomatyzowany ma ona prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego swoje dane osobowe.

2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

3. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

4. Wykonanie prawa, o którym mowa w ust. 1, pozostaje bez uszczerbku dla prawa do usunięcia danych.

5. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Rozdział VI. Prawo do wniesienia sprzeciwu wobec przetwarzania danych

1. Jeżeli przetwarzanie oparte jest na przesłance wykonania zadania realizowanego w interesie publicznym lub prawnie uzasadnionym interesie administratora, osoba, której dane dotyczą z przyczyn związanych z jej szczególną sytuacją, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych osobowych.

2. Administratorowi nie wolno już przetwarzać danych osobowych, względem których wniesiono sprzeciw, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

3. W momencie złożenia sprzeciwu wobec przetwarzania administrator niezwłocznie ogranicza przetwarzanie i weryfikuje czy istnieją ważniejsze uzasadnione podstawy do przetwarzania niż interes osoby wnioskującej. Jeżeli administrator posiada podstawę prawną, o której mowa powyżej, informuje osobę wnioskującą o odmowie realizacji prawa wraz z uzasadnieniem decyzji. W przypadku, gdy uzasadniona jest przesłanka do zrealizowania żądania, postępuje się zgodnie z ust. 2.

4. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

5. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Rozdział VII Prawo do niepodlegania decyzjom na podstawie zautomatyzowanego przetwarzania

1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

2. To prawo nie ma zastosowania, jeżeli ta decyzja:

jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem

jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą

opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

przetwarzane są jej dane osobowe.

Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz pozyskania następujących informacji:

1) w jakim celu są przetwarzane
2) jakich kategorii danych osobowych dotyczy przetwarzanie;
3) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) o planowanym okresie przechowywania danych osobowych, a gdy nie jest możliwe wskazanie konkretnego czasu przechowywania, o kryteriach ustalania tego okresu;
5) o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) o prawie wniesienia skargi do organu nadzorczego;
7) o źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą.

2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

3. Jeżeli osoba, której dane dotyczą, zwróci się z wnioskiem o dostarczenie kopii jej danych osobowych podlegających przetwarzaniu, żądanie takie realizuje się bezpłatnie. Za wszelkie kolejne kopie, można pobrać opłatę. Opłata powinna obejmować jedynie faktyczne koszty sporządzenia kopii, tj. koszt papieru, koszty kserowania. Cennik może być ustalony odrębnie dla każdej komórki organizacyjnej lub sporządzony dla całej jednostki.

4. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną po jednoznacznej weryfikacji tożsamości osoby, np. podaniu daty urodzenia, podaniu innej informacji, która była podana we wcześniejszej korespondencji, a co do której można mieć pewność, że będzie ją posiadać jedynie osoba, którego dane dotyczą.

5. Kopię danych, o której mowa w ust. 3, wydaje się w postaci wydruku po ich przepisaniu lub skopiowaniu do ustrukturyzowanego powszechnie używanego formatu nadającego się do odczytu maszynowego (informacja maszynowa). Nie wydaje się skanów dokumentów ani ich kserokopii, które mogą zawierać dodatkowe dane niedotyczące osoby występującej z wnioskiem.

6. Prawo do uzyskania kopii, nie może niekorzystnie wpływać na prawa i wolności innych.

7. Inspektor ochrony danych wraz z pracownikiem merytorycznym, realizującym wniosek, podejmują decyzję, czy kopię danych wydać w postaci zanonimizowanych kopii dokumentów i/lub plików, czy informacji przetworzonej o kategoriach przetwarzanych danych. Prawo do uzyskania kopii danych, nie jest równoważne z prawem do uzyskania kopii dokumentów lub plików, w których te dane są zawarte.

Załącznik nr 15

PROCEDURA UDOSTĘPNIANIA DANYCH OSOBOWYCH

I. Cel: opis sposobu postępowania przy zgłaszaniu żądania o udostępnienie danych osobowych na wniosek innego podmiotu.

II. Osoby odpowiedzialne : wszyscy pracownicy upoważnieni przez Administratora

III. Zasady ogólne:

1. Procedura określa zasady przekazywania danych osobowych na wniosek innego podmiotu.
2. Udostępnienie jest szczególnym rodzajem przekazania danych innemu podmiotowi w wyniku, którego staje się on odrębnym administratorem danych.
3. Podstawą udostępnienia danych może być:
   * zgoda (udokumentowana) osoby, której danych dotyczą na udostępnienie jej danych;
   * przepis prawa, który wymaga udostępnienia;
   * prawnie uzasadnionego interesu wnioskodawcy;
   * konieczność zrealizowania umowy, której stroną jest osoba, której dane dotyczą.
4. Zgoda osoby, której dane dotyczą może służyć udostępnieniu, np. udostępnieniu przez pracodawcę firmie oferującej benefity danych pracownika, w celu umożliwienia zawarcia z nim umowy.
5. Udostępnienie w związku z obowiązkiem wynikającym z przepisów prawa, wymaga wskazania przez wnioskodawcę zarówno szczegółowego przepisu w randzie ustawy (tzn. ustawa oraz jej konkretne artykuły), a także celu i zakresu danych, które mają podlegać udostępnieniu. Najczęściej udostępnienie będzie następować na wniosek policji, sądu, prokuratury, komornika lub pomocy społecznej.
6. Prawnie uzasadniony interes wnioskodawcy, wskazany we wniosku o udostępnienie, wymaga wykazania, że ten interes jest faktyczny. Wnioskodawca musi także wykazać, że udostępnienie danych w tym celu jest niezbędne do jego zrealizowania, a także że jego interes przewyższa interesy osoby lub osób, których danych chce uzyskać.
7. Niektóre umowy wymagają udostępnienia danych osoby, z którą została zawarta, np. umowa konsumencka zawarta w związku z zakupem w sklepie internetowym wymaga udostępnienia danych operatorowi elektronicznych płatności, czy dostawcom zamówienia.
8. Przepisy o ochronie danych osobowych nie określają wzoru wniosku o udostępnienie, na potrzeby niniejszej procedury wprowadzono wewnętrzny wzór wniosku, który można udostępnić wnioskodawcy.
9. Wnioskodawca może przekazać żądanie, korzystając ze swojego wzoru wniosku, z zastrzeżeniem, że jego wniosek musi zawierać elementy umożliwiające dokonanie oceny zasadności wniosku.
10. Wymagane elementy wniosku o udostępnienie:
    * dane podmiotu, który wnioskuje o uzyskanie danych;
    * wskazanie podstawy udostępnienia;
    * wskazanie osoby, której dane dotyczą;
    * zakres danych, których ma dotyczyć udostępnienie;
    * cel udostępnienia;
    * podpis i dane osoby działającej w imieniu składającego wniosek.
11. W przypadku wniosku przekazywanego drogą elektroniczną, wnioskodawca może podpisać wniosek podpisem elektronicznym (kwalifikowanym lub profilem zaufanym).

IV. Postępowanie w przypadku otrzymania wniosku o udostępnienie danych:

1. O otrzymanym wniosku należy niezwłocznie poinformować IOD, który udzieli wsparcia w ocenie jego zasadności oraz realizacji.
2. W przypadku otrzymania żądania w formie ustnej, w treści wiadomości e-mail, poprzez komunikator internetowy, itp. należy poinformować wnioskodawcę o konieczności sformalizowania wniosku o udostępnienie danych, aby zawierał informacje wymagane zgodnie z punktem 1) ust. 10 Procedury oraz podpis wnioskodawcy i udostępnić wnioskodawcy przykładowy wzór wniosku o udostępnienie (załącznik nr 1 do Procedury).
3. W przypadku otrzymania wniosku we właściwej formie, należy dokonać weryfikacji elementów wniosku z punktem 1 ust. 10, w szczególności:
   * Czy zostały precyzyjnie wskazane dane podmiotu, który wnioskuje o uzyskanie danych, tzn.
     - nazwa, adres, dane rejestrowe; lub
     - w przypadku osoby fizycznej imię, nazwisko, numer i seria dokumentu tożsamości lub PESEL?
   * Czy została wskazana podstawa udostępnienia, tzn.
     - przepis prawa w randze ustawy oraz konkretne artykuły tego przepisu; lub
     - prawnie uzasadniony interes administratora z uzasadnieniem niezbędności udostępnienia danych?
   * Czy zostały wskazane osoby, do których odnosi się wniosek, tzn.
     - we wniosku określono wystarczająco precyzyjnie, czyje dane mają podlegać udostępnieniu?
   * Czy został określony zakres danych, których ma dotyczyć udostępnienie?
   * Czy został wskazany cel udostępnienia i jest on zgodny z podstawą prawną wskazaną we wniosku?
   * Czy wniosek zawiera podpis i dane osoby działającej w imieniu składającego wniosek?
4. W przypadku stwierdzenia braków we wniosku, należy niezwłocznie skontaktować się z wnioskodawcą i poinformować go o konieczności uzupełnienia wniosku. Dopuszczalny jest kontakt telefoniczny lub z wykorzystaniem poczty e-mail, w celu przyśpieszenia procedury udostępnienia danych.
5. Jeżeli wnioskodawca nie udzieli odpowiedzi/dodatkowych wyjaśnień, należy pozostawić wniosek bez rozpatrzenia, a po upływie 30 dniu przekazać decyzję o odmowie udostępnienia danych ze względu na błędy formalne we wniosku.
6. W przypadku stwierdzenia, że wskazany we wniosku prawnie uzasadniony interes wnioskodawcy nie jest rzeczywisty lub udostępnienie danych nie jest niezbędne do zrealizowania wskazanych celów, należy odmówić udostępnienia danych, wskazując na niewystarczające uzasadnienie prawnego interesu wnioskodawcy.
7. W przypadku powołania się na przepis prawa, należy dokonać weryfikacji podanego we wniosku przepisu prawa, tzn.
   - Czy wskazany przepis prawa istnieje i jest obowiązujący?
   - Czy przepis jest w randze ustawy?
   - Czy treść przywołanego przepisu faktycznie uprawnia wnioskodawcę do żądania udostępnienia danych?
   - Czy wskazany we wniosku cel przetwarzania jest spójny z celem wskazanym w przepisie?
8. Jeżeli wnioskodawca powołał się na przepis prawa, jednakże nie wskazał jego konkretnych artykułów, należy wezwać go do uszczegółowienia podstawy prawnej. Nie można udostępnić danych na podstawie przypuszczenia, że wskazany przepis faktycznie uprawnia wnioskodawcę do otrzymania danych.

9. Jeżeli wnioskodawca wskazał nieobowiązujący już przepis prawa lub przepis w randze rozporządzenia, należy wezwać go do wskazania właściwej podstawy prawnej.
10. Jeżeli wnioskodawca wskazał we wniosku cel udostępnienia niezgodny z celami, dla których dopuszcza możliwość udostępnienia danych wskazany przez niego przepis, należy poinformować wnioskodawcę o braku możliwości zrealizowania żądania udostępnienia ze względu na rozbieżność wskazanych celów i podstawy udostępnienia.
11. Jeżeli wskazany we wniosku przepis prawa nie uprawnia do udostępnienia danych, należy poinformować wnioskodawcę o braku możliwości zrealizowania żądania udostępnienia.
12. Jeżeli wskazany we wniosku zakres danych jest zbyt szeroki w odniesieniu do wskazanej przez wnioskodawcę podstawy prawnej, należy zwrócić się do wnioskodawcy o uzupełnienie podstawy prawnej lub zmianę zakresu żądanych danych. Do czasu udzielenia wyjaśnień, wniosek pozostaje bez rozpatrzenia. Po 30 dniach od wysłania dodatkowych pytań i braku uzyskania odpowiedzi, należy rozpatrzyć wniosek negatywnie.
13. W przypadku pozytywnej oceny wniosku, należy przekazać wniosek wraz z decyzją o udostępnieniu danych do inspektora ochrony danych oraz kierownictwa, w celu zatwierdzenia udostępnienia.
14. Udostępnienie danych następuje w formie jakiej zażądał wnioskodawca, a w przypadku braku wskazania formy udostępnienia, jest realizowane w formie w jakiej został złożony wniosek.
15. Udostępnienie danych następuje z zastrzeżeniem konieczności zapewnienia ich poufności w czasie przekazania, tzn.
    * w przypadku przekazywania drogą elektroniczną, należy dane zapisać w pliku zabezpieczonym hasłem, które zostanie przekazane wnioskodawcy ustaloną drogą komunikacji (nigdy w treści wiadomości zawierającej załącznik);
    * w przypadku przekazywania drogą pocztową, należy zastosować dwie koperty, gdzie na wewnętrznej zostanie dodany dopisek "do rąk własnych .....". Przesyłka pocztowa musi być rejestrowana i wysłana za potwierdzeniem odbioru;
    * osobistego odbioru, należy dokonać weryfikacji tożsamości wnioskodawcy poprzez okazanie dowodu osobistego. Przekazanie danych odbywa się za pokwitowaniem, gdzie wnioskodawca wskazuje swoje imię, nazwisko, datę odbioru i potwierdza podpisem odebranie danych.
16. Udostępnienie danych należy odnotować w wewnętrznym rejestrze (załącznik nr 2 do Procedury).
17. Wniosek o udostępnienie wraz z decyzją o sposobie realizacji wniosku, w formie adnotacji dokonanej przez osobę odpowiedzialną za rozpatrzenie wniosku, należy przechowywać przez okres 10 lat po zrealizowaniu wniosku.

Załącznik nr 1 WZÓR – WNIOSEK O UDOSTĘPNIENIE DANYCH

Dane wnioskodawcy:

Nazwa wnioskodawcy lub jego imię i nazwisko:* .....

Adres:*.....

PESEL/REGON:*..... Telefon: ..... i/lub e-mail: .....

Wnioskuję o udostępnienie danych osoby/osób:

.....

W zakresie: .....

W celu: .....

Uzasadnienie wniosku (wskazanie podstawy prawnej udostępnienia):

.....

Data i podpis wnioskodawcy .....

Imię i nazwisko osoby działającej w imieniu wnioskodawcy: .....

Klauzula informacyjna dla wnioskodawcy lub osób, działających w jego imieniu

Zgodnie z art. 13 ust. 1 i ust. 2 rozporządzenia 2016/679 (RODO), informujemy, iż:

- Administratorem moich danych osobowych podanych w formularzu oraz dokumentach rekrutacyjnych jest: ***Szkoła Podstawowa Nr 2 im. bł. Edmunda Bojanowskiego w Woli Rzędzińskiej, 33-150 Wola Rzędzińska 253a,*** *e-mail:* ***kontakt@szpwola.pl****, nr tel.:* ***146792124***
- W sprawach dotyczących przetwarzania danych, w tym skorzystania z przysługujących na mocy przepisów RODO praw, może Pan/i skorzystać ze wskazanych danych kontaktowych lub skontaktować się z inspektorem ochrony danych: za pośrednictwem poczty elektronicznej: ***firma.tomaszpilch@onet.pl*** lub pisemnie na adres siedziby administratora.
- Pani/a dane osobowe będą przetwarzane w związku z realizowaniem otrzymanego wniosku, a także w celu obrony przed roszczeniami powstałymi w związku z realizacją wniosku, na podstawie naszego prawnie uzasadnionego interesu.
- Odbiorcami Pani/a danych osobowych będą podmioty upoważnione do tego na podstawie przepisów prawa, a także kancelarie prawne, operatorzy pocztowi, firmy kurierskie.
- Posiada Pan/i prawo żądania dostępu do swoich danych osobowych, a także ich sprostowania (poprawiania). Przysługuje Pani/u także prawo do żądania usunięcia lub ograniczenia przetwarzania, przenoszenia danych, a także sprzeciwu na przetwarzanie, przy czym przysługuje ono jedynie w sytuacji, jeżeli dalsze przetwarzanie nie jest niezbędne do wywiązania się przez Administratora z obowiązku prawnego i nie występują inne nadrzędne prawne podstawy przetwarzania.
- Ma Pani/Pan prawo wniesienia skargi na sposób przetwarzania przez administratora do Prezesa UODO pisząc na adres: Urząd Ochrony Danych Osobowych ul. Stawki 2, 00-193 Warszawa, ***www.uodo.gov.pl.***
- Podanie danych jest dobrowolne, ale niezbędne do zrealizowania wniosku.
- Pani/Pana dane nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

Załącznik nr 2 REJESTR ODNOTOWYWANIA INFORMACJI O ODBIORCACH DANYCH

Nr	Wnioskodawca	Podstawa prawna wskazana we wniosku	Data wniosku	Pracownik rozpatrujący wniosek	Data udostępnienia	Informacja o zakresie udostępnienia