# POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

# DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH

w

Szkole Podstawowej im. Marii Konopnickiej

w Harkabuzie

# SPIS TREŚCI

# 1. WPROWADZENIE

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich ochrony w Szkole Podstawowej im. Marii Konopnickiej w Harkabuzie z siedzibą Harkabuz 47 zwanym dalej **SZKOŁĄ.**

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

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

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

# 2. PODSTAWY PRAWNE

## 2.1. USTAWA ORAZ AKTY WYKONAWCZE

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

- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926)
- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2006, Nr 203, poz. 1494) – art. 13.3 ustawy
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz. 923) – art. 22a ustawy
- 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) – art. 39a ustawy
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536) – art. 46a ustawy.

Niniejszy dokument powstał w oparciu o **art. 36 ust. 2 oraz 39a ustawy o ochronie danych osobowych**, które zobowiązują Administratora danych do wykonania dokumentacji opisującej środki organizacyjne i techniczne służące ochronie przetwarzanych danych osobowych.

Szczegółowy zakres dokumentu określa 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 wydane do art. 39a ustawy.

## 2.2. DEFINICJE

W dokumencie przyjmuje się następującą terminologię:

**Generalny Inspektor Ochrony Danych Osobowych** – organ do spraw ochrony danych osobowych.

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

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

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

**Administrator bezpieczeństwa informacji (ABI)** – osoba nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

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

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

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

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

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

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

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

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

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

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

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

# 3. NAJWAŻNIEJSZE ZAGADNIENIA OCHRONY DANYCH OSOBOWYCH

## 3.1. GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

**Zadania GIODO**

Do zadań GIODO należy:

- kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych,
- prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach,
- opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,
- inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
- uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

**Kontrole GIODO**

W celu wykonania w/w zadań Generalny Inspektor, zastępca Generalnego Inspektora lub upoważnieni przez niego pracownicy Biura, zwani dalej „inspektorami”, mają prawo:

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

**Działania GIODO w przypadku naruszenie przepisów**

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

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

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

## 3.2. PRZETWARZANIE DANYCH

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

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

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

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

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

## 3.3. OBOWIĄZKI INFORMACYJNE O PRZETWARZANIU DANYCH

**Zbieranie danych osobowych od osób, których dane dotyczą**

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

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy Administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- prawie dostępu do treści swoich danych oraz ich poprawiania,
- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Podanych wyżej zasad **nie stosuje się**, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

**Zbieranie danych osobowych nie od osób, których dane dotyczą.**

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

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

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

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

## 3.4. OBOWIĄZEK ZGŁOSZENIA PRZETWARZANIA DANYCH

Administrator danych jest **obowiązany** zgłosić zbiory danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz zgłaszać zmiany w terminie 30 dni. Zgłoszenie powinno zawierać:

- wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych,
- oznaczenie podmiotu prowadzącego zbiór i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru,
- cel przetwarzania danych, w tym opis kategorii osób, których dane dotyczą oraz zakres przetwarzanych danych,
- sposób zbierania oraz udostępniania danych, w tym informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane,
- opis środków technicznych i organizacyjnych zastosowanych w celach ochrony danych,
- informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w dokumentacji ochrony danych osobowych,
- informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

Z obowiązku rejestracji **zwolnieni są** Administratorzy danych:

- objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności,
- przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym oraz przetwarzanych przez Generalnego Inspektora Informacji Finansowej, a także przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej,
- dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego,
- przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,
- dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,
- tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na Urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego,
- dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności,
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
- powszechnie dostępnych,
- przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,
- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

## 3.5. UDOSTĘPNIANIE DANYCH

Najważniejsze przesłanki i zasady udostępniania danych:

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

- Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

## 3.6. POWIERZENIE PRZETWARZANIA DANYCH

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

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

Do kontroli zgodności przetwarzania danych przez podmiot, któremu powierzono przetwarzanie danych, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19 ustawy.

## 3.7. DOKUMENTOWANIE

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

Ponadto, Administrator danych:

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

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

## 3.8. SANKCJE KARNE

- Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie **nie jest dopuszczalne** albo do których przetwarzania **nie jest uprawniony**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **lat 2**. Jeżeli czyn ten dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **lat 3**.
- Kto administrując zbiorem danych przechowuje w zbiorze dane osobowe **niezgodnie z celem utworzenia zbioru**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.
- Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych **udostępnia je lub umożliwia dostęp** do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **lat 2**. Jeżeli sprawca działa **nieumyślnie**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.
- Kto administrując danymi **narusza choćby nieumyślnie obowiązek zabezpieczenia** ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.
- Kto będąc do tego obowiązany **nie zgłasza do rejestracji zbioru danych**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.
- Kto administrując zbiorem danych **nie dopełnia obowiązku poinformowania osoby, której dane dotyczą**, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.
- Wobec osoby, która w przypadku naruszenia zasad bezpieczeństwa lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonych w niniejszej dokumentacji, 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**.
- Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie **obowiązków pracowniczych**.
- Orzeczona kara dyscyplinarna **nie wyklucza odpowiedzialności karnej** osoby winnej zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, póz. 926) oraz możliwości wniesienia wobec niej sprawy z **powództwa cywilnego** przez pracodawcę o zrekompensowanie poniesionych strat.

# 4. ZAGROŻENIA BEZPIECZEŃSTWA

## 4.1. CHARAKTERYSTYKA MOŻLIWYCH ZAGROŻEŃ

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

## 4.2. SYTUACJE ŚWIADCZĄCE O NARUSZENIU ZASAD BEZPIECZEŃSTWA

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

- **ujawnienie istnienia nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki”, itp.,
- **podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowania lub kopiowanie danych,
- **rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji** (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

## 4.3. TABELE FORM NARUSZENIA BEZPIECZEŃSTWA I SPOSOBY POSTĘPOWANIA

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

| FORMY NARUSZEŃ | SPOSOBY POSTĘPOWANIA |
|---|---|
| **W ZAKRESIE WIEDZY** | |
| Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym. | Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić administratora bezpieczeństwa informacji. |
| Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej. | |
| Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji. | |
| **W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA** | |
| Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych. | Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport |
| Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony. | Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport. |
| Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci. | Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport. |
| Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym. | Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport. |
| Samodzielne instalowanie jakiegokolwiek oprogramowania. | Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport. |
| Modyfikowanie parametrów systemu i aplikacji. | Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Sporządzić raport. |

| | |
|---|---|
| Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym. | Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport. |
| **W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE** | |
| Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru. | Zabezpieczyć dokumenty. Sporządzić raport. |
| Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych. | Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport. |
| Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie. | Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport. |
| Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią. | Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport. |
| Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe. | Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport |
| Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą. | Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport. |
| Utrata kontroli nad kopią danych osobowych. | Podjąć próbę odzyskania kopii. Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport. |
| **W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH** | |
| Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych. | Zabezpieczyć pomieszczenie. Powiadomić przełożonych. Sporządzić raport. |
| Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym. | Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i administratora bezpieczeństwa informacji. Sporządzić raport. |
| Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji. | Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport. |
| **W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI** | |
| Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy | Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby |

| | |
|---|---|
| urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.). | informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport. |
| Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych. | Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport. |

**Tabela zjawisk świadczących o możliwości naruszenia ochrony danych osobowych**

| FORMY NARUSZEŃ | SPOSOBY POSTĘPOWANIA |
|---|---|
| Ślady manipulacji przy układach sieci komputerowej lub komputerach. | Powiadomić niezwłocznie administratora bezpieczeństwa informacji oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport. |
| Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu. | Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport. |
| Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych. | |
| Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych. | |
| Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania. | |
| Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe. | Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie administratora bezpieczeństwa informacji. Sporządzić raport. |

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

| FORMY NARUSZEŃ | SPOSOBY POSTĘPOWANIA |
|---|---|
| Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej. | Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport. |
| Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika. | |

# 5. POLITYKA BEZPIECZEŃSTWA

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

## 5.1. DEKLARACJA

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

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

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

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

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

## 5.2. CHARAKTERYSTYKA INSTYTUCJI

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

## 5.3. WYKAZ ZBIORÓW OSOBOWYCH

Na podstawie § 4 pkt 2 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 **tworzy się wykaz zbiorów osobowych wraz ze wskazaniem programów komputerowych** służących do ich przetwarzania zgodnie z **załącznikiem nr 1** do niniejszej dokumentacji.

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

## 5.4. WYKAZ MIEJSC PRZETWARZANIA

Na podstawie § 4 pkt 1 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 tworzy się wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych.

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

## 5.5. EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z art. 39 ust. 1 ustawy o ochronie danych osobowych wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi **załącznik nr 3** do niniejszej dokumentacji.

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

Ewidencja stanowi podstawę wydania Upoważnienia do przetwarzania danych osobowych na mocy art. 37 ustawy o ochronie danych osobowych.

## 5.6. ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

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

- Przetwarzanie danych osobowych w Szkole może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- Zgodnie z art. 36 ust. 3 ustawy o ochronie danych osobowych, Administrator danych **powołuje Administratora bezpieczeństwa informacji.**
- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne **upoważnienie**. Wzór upoważnienia stanowi **załącznik nr 4** do niniejszej dokumentacji.
- ABI prowadzi **ewidencję osób upoważnionych,** o której mowa w pkt 5.5 oraz na jej podstawie przygotowuje **Upoważnienia do przetwarzania danych** i przedkłada je do podpisu ADO.
- Unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego **załącznik nr 5** do niniejszej dokumentacji.
- Zabrania się przetwarzania danych poza obszarem określonym w załączniku nr 2 do niniejszej instrukcji.
- Każdy pracownik Szkoły co najmniej raz na 2 lata musi odbyć **szkolenie z zakresu ochrony danych** osobowych. Za organizację szkoleń odpowiedzialny jest ABI, który prowadzi w tym celu odpowiednią dokumentację. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.

- Ponadto każdy upoważniony do przetwarzania danych **potwierdza pisemnie** fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi **załącznik nr 6** do niniejszej dokumentacji. Podpisany dokument jest dołączany do akt osobowych.
- Obszar przetwarzania danych osobowych określony w załączniku nr 2 do niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
- Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych. Wzory zgody na przebywanie w pomieszczeniach dla osób nie posiadających upoważnienia, a także odwołania tej zgody, stanowią odpowiednio **załącznik nr 7** oraz **załącznik nr 8** do przedmiotowej dokumentacji.
- Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
- Przetwarzanie danych podawanych dobrowolnie może odbywać się tylko na podstawie pisemnej zgody podającego te dane wg wzoru określonego w **załączniku nr 10.**

Dla zapewnienia kontroli przestrzegania zasad określonych w niniejszej dokumentacji wyznacza się następujące **zadania Administratorowi bezpieczeństwa informacji:**

- Nadzór nad przetwarzaniem danych zgodnie z ustawą o ochronie danych osobowych i innymi przepisami prawa.
- Kontrola przestrzegania zasad ochrony – systematycznie, nie rzadziej niż dwa razy do roku kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w szczególności:
    - Kontrola dokumentacji opisującej sposób przetwarzania oraz ochrony.
    - Kontrola fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są informacje.
    - Kontrola poprawności zabezpieczeń danych przetwarzanych metodami tradycyjnymi.
    - Kontrola awaryjnego zasilania komputerów.
    - Nadzór nad naprawą, konserwacją oraz likwidacją urządzeń komputerowych.
    - Kontrola systemu kontroli obecności wirusów komputerowych.
    - Kontrola wykonywania kopii awaryjnych.
    - Kontrola przeglądu, konserwacji oraz uaktualnienia systemów informatycznych.
    - Kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych.

- Kontrola nadanych upoważnień.

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

## 5.7. ŚRODKI TECHNICZNE OCHRONY DANYCH OSOBOWYCH

Zbiory danych przetwarzane w Szkole zabezpiecza się poprzez:

1. Środki ochrony fizycznej.
   - Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie .
   - Zbiory danych osobowych przechowywane są w pomieszczeniach, w których okna zabezpieczone są za pomocą , rolet.
   - Pomieszczenia, w którym przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
   - Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie.
   - Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
   - Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
2. Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej.
   - Zbiory danych osobowych przetwarzane są przy użyciu komputera stacjonarnego i przenośnego .
   - Komputer służący do przetwarzania danych osobowych jest połączony z lokalną siecią komputerową.
   - Zastosowano urządzenia typu UPS, i wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
   - Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
   - Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
   - Użyto system Firewall do ochrony dostępu do sieci komputerowej.

3. **Środki ochrony w ramach systemowych narzędzi programowych i baz danych.**
   - Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

- Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
- Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

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

# 6. ZAŁĄCZNIKI

Załącznik nr 1. Wykaz zbiorów osobowych przetwarzanych w Szkole.

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

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

Załącznik nr 4. Wzór upoważnienia do przetwarzania danych osobowych.

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

Załącznik nr 6. Wzór potwierdzenia znajomości zasad bezpieczeństwa.

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

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

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

Załącznik nr 10. Wzór zgody na przetwarzanie danych.

# WYKAZ ZBIORÓW OSOBOWYCH

| Lp. | Nazwa zbioru - opis<br>DOKUMENTACJA SŁUŻĄCA DO PRZETWARZANIA ZBIORU DANYCH<br>Nazwa zbioru - opis | Struktura zbioru | Systemy informatyczne | MIEJSCE PRZETWARZANIA /ODPOWIEDZIALNY/ | Zastosowany Poziom bezpieczeństwa | Zgłoszenie GIODO |
|---|---|---|---|---|---|---|
| 1. | | | | | | |
| 2. | | | | | | |
| 3. | | | | | | |
| 4. | | | | | | |
| 5. | | | | | | |
| 6. | | | | | | |
| 7. | | | | | | |
| 8. | | | | | | |
| 9. | | | | | | |
| 10. | | | | | | |
| 11. | | | | | | |
| 12. | | | | | | |
| 13. | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 14. | | | | | | |
| 15. | | | | | | |

# WYKAZ MIEJSC PRZETWARZNIA DANYCH OSOBOWYCH

| Lp. | Nazwa pomieszczenia | Adres |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |
| 11 | | |
| 12 | | |
| 13 | | |

# EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

| Lp. | Nazwisko, Imię | Nr zbiorów | Okres upoważnienia | | Program/identyfikator | Uwagi |
|---|---|---|---|---|---|---|
| | | | OD | DO | | |
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |
| 7 | | | | | | |
| 8 | | | | | | |
| 9 | | | | | | |
| 10 | | | | | | |
| 11 | | | | | | |
| 11 | | | | | | |
| 12 | | | | | | |
| 13 | | | | | | |
| 14 | | | | | | |

……, dn. ……

……

**WAŻNOŚĆ**

od: ……..

do: ***do odwołania***

# UPOWAŻNIENIE

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101 poz. 926, ze zm.) upoważniam Panią/Pana:

**.....**

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

| Nr zbiorów z ewidencji zbiorów | Nazwa programu / identyfikator |
|---|---|
| | |

……
(podpis Administratora danych)

……., dn. ……

……

# UNIEWAŻNIENIE

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101 poz. 926, ze zm.) unieważniam upoważnienie do przetwarzania danych osobowych wydane dnia ……dla Pani/Pana:……

**……..**

……
(podpis Administratora danych)

……., dn. ……

…….

(imię i nazwisko pracownika)

**OŚWIADCZENIE**

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść:

   a) Dokumentacji ochrony danych osobowych w Szkole Podstawowej Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926),
   b) 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).

2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy, a w szczególności nie będę:

   a) ujawniać danych zawartych w eksploatowanych w systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
   b) ujawniać szczegółów technologicznych używanych w systemów oraz oprogramowania,
   c) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
   d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą Dokumentacją.

…….  ……

(podpis pracownika)  (podpis przełożonego)

……, dn. ……

……

**WAŻNOŚĆ**

od: ……

do: ……

# ZGODA

## NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie pkt I.2 załącznika do 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. z 2004 r. Nr 100, poz. 1024 z późn. zm.), **wyrażam zgodę Pani/Panu:**

**……**

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

……
(podpis Administratora danych)

……, dn. ……

……

# ODWOŁANIE ZGODY
## NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie pkt I.2 załącznika do 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. z 2004 r. Nr 100, poz. 1024 z późn. zm.), **odwołuję zgodę** z dnia …….. o sygnaturze …… udzieloną **Pani/Panu:**

**……..**

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

……
(podpis Administratora danych)

**RAPORT**
**z naruszenia bezpieczeństwa zasad ochrony danych osobowych**
**w ……**

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

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

3. Lokalizacja zdarzenia:

……
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……
……
……

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

6. Podjęte działania:
……
……
……

7. Postępowanie wyjaśniające:
……
……
……

……
(data, podpis Administrator danych)

……, dn. ……

……
(imię i nazwisko, adres zamieszkania)

## ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Na podstawie art. 23 ust.1 pkt 1 (oraz/lub art. 27.2 pkt 1 – dla danych wrażliwych) ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926), wyrażam zgodę na przetwarzanie niżej wymienionych moich danych osobowych.

Zgoda udzielona jest tylko do przetwarzania danych oraz ich udostępniania w podanym niżej zakresie.

| Lp. | Zakres danych – zgoda | Cel przetwarzania | Odbiorcy lub kategorie odbiorców danych |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| … | | | |

Jednocześnie zgodnie z art. 24 ust. 1 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926) przyjmuję do wiadomości, że:

- Administratorem danych jest …… z siedzibą .....,
- dane będą przetwarzane wyłączenie zgodnie z określonym celem,
- dane będą udostępniane wyłącznie podanym odbiorcom,
- przysługuje mi prawo dostępu do treści danych oraz ich poprawiania,
- dane podaję dobrowolnie.

……

(podpis)