

**PROCEDURA POLITYKI BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH
OBOWIĄZUJĄCA W ZESPOLE SZKÓŁ NR 4
IM. MARYNARKI WOJENNEJ RP
W WOŁOMINIE**

Podstawa prawna:

Ustawę z dn. 29.08.1997 r. o ochronie danych osobowych (ze zm.),

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3.06.1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia Inspektora Ochrony Danych Osobowych (ze zm.),

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych,

I. USTALENIA WSTĘPNE

§ 1

Dyrektor szkoły w zakresie ochrony danych osobowych oświadcza, że w szkole:

- 1) podejmuje się działania dla ochrony praw związanych z bezpieczeństwem danych osobowych,
- 2) podnosi się świadomość oraz kwalifikacje osób przetwarzających dane osobowe w zakresie problematyki bezpieczeństwa tych danych,
- 3) ochrona danych osobowych należy do podstawowych obowiązków pracowniczych,
- 4) obowiązek ochrony danych będzie egzekwowany od każdego pracownika, który w jakikolwiek sposób ma do nich dostęp.

§ 2

1. Dyrektor jest świadomy zagrożeń związanych z przetwarzaniem danych w szczególności wynikających z dynamicznego rozwoju metod i technik przetwarzania danych w systemach informatycznych oraz sieciach telekomunikacyjnych.
2. Dyrektor zamierza doskonalić i rozwijać nowoczesne metody przetwarzania danych.
3. Dyrektor szkoły deklaruje, że szkoła będzie doskonaliła i rozwijała możliwe środki ochrony danych osobowych w celu skutecznego zapobiegania zagrożeniom wykradania zasobów komputerowych:
 - a) związanych z: wirusami, spamami, stronami i komunikatorami internetowymi,
 - b) użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania pliku poza szkołę,
 - c) możliwością niekontrolowanego kopiowania danych na zewnętrzne, przenośne nośniki,
 - d) możliwością podsłuchiwania sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochroną dane,
 - e) lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia,
 - f) brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy,
 - g) atakami z sieci uniemożliwiającymi przetwarzanie,
 - h) kradzieżą sprzętu lub nośników z danymi,
 - i) przekazywaniem sprzętu z danymi do serwisu,
 - j) innym możliwym zagrożeniom.

§ 3

1. Dane osobowe gromadzone są oraz przetwarzane z przestrzeganiem obowiązujących przepisów prawa.
2. Dane osobowe przetwarzane są w celu realizacji statutowych celów szkoły dla realizacji:
 - a) zadań dydaktycznych, wychowawczych, opiekuńczych i organizacyjnych wynikających z ustawy z 7.09.1991 r. o systemie oświaty,
 - b) polityki kadrowej oraz bieżącej obsługi stosunków pracy i zatrudnienia.

§ 4

Polityka bezpieczeństwa danych osobowych dotyczy danych gromadzonych i przetwarzanych w zbiorach:

- 1) drukowanych znajdujących się w kartotekach, skorowidzach, księgach, we wszystkich zbiorach ewidencyjnych,
- 2) w systemach informatycznych.

§ 5

1. Szkoła chroni wszystkie posiadane zasoby zgodnie z ww. przepisami prawa.
2. Pod szczególną ochroną są tzw. wrażliwe dane osobowe wymienione w art. 27 ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych.
3. Przetwarzanie danych ujawniających:
 - a) pochodzenie rasowe lub etniczne,
 - b) poglądy polityczne, przekonania religijne lub filozoficzne,
 - c) przynależność wyznaniową, partyjną lub związkową, jak również
 - d) danych o stanie zdrowia,
 - e) kodzie genetycznym, nałogach lub życiu seksualnym oraz
 - f) danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnymdopuszczalne jest tylko w związku z realizacją celów statutowych szkoły i w granicach wynikających z przepisów art. 27 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych.

§ 6

1. Szkoła stosuje środki informatyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczając dane przed:
 - a) ich udostępnieniem lub zabraniem przez osobę nieuprawnioną,
 - b) zmianą, utratą, uszkodzeniem lub zniszczeniem,
 - c) przetwarzaniem z naruszeniem ustawy.
2. Szkoła unowocześnia oraz zapewnia aktualizacje informatycznych środków ochrony danych osobowych pozwalającą na zabezpieczenie przed wirusami, nieuprawnionym dostępem oraz inni zagrożeniami danych, płynącymi z funkcjonowania systemu informatycznego oraz sieci telekomunikacyjnych.

§ 7

1. Szkoła sprawuje kontrole i nadzór nad niszczeniem zbędnych danych osobowych, ich zbiorów.
2. Niszczenie tych danych osobowych, ich zbiorów polega na:
 - a) trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod,
 - b) anonimizacji danych osobowych, zbiorów polegającej na pozbawieniu danych osobowych, ich zbiorów – cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.
3. Naruszenie przez zatrudnione osoby w ramach stosunku pracy, upoważnione do dostępu i przetwarzania danych osobowych stosowanych procedur niszczenia zbędnych danych osobowych, ich zbiorów traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków pracowniczych ze wszystkimi konsekwencjami, włącznie z rozwiązaniem stosunku pracy.
4. Kontrola i nadzór nad niszczeniem zbędnych danych osobowych, ich zbiorów może polegać na wprowadzeniu odpowiednich procedur niszczenia danych, a także zleceniu niszczenia ich, wyspecjalizowanym podmiotom zewnętrznym, gwarantującym bezpieczeństwo procesu niszczenia danych odpowiednie do rodzaju nośnika tych danych.

§ 8

1. Szkoła prowadzi dokumentację określającą sposób przetwarzania danych oraz środki ochrony tych danych, którą jest niniejsza procedura.
2. Załącznikami do niniejszej procedury są:
 - 1) rejestr upoważnień dostępu do danych osobowych oraz ich przetwarzania ,
 - 2) upoważnienie dla pracownika do dostępu i przetwarzania danych ,
 - 3) oświadczenie o zapoznaniu się pracownika z przepisami o ochronie danych ,
 - 4) oświadczenie o wyrażeniu zgody na gromadzenie i przetwarzanie danych.
3. Zarządzenia Dyrektora w zakresie polityki bezpieczeństwa danych osobowych mogą dotyczyć:
 - 1) instrukcji sposobu i formy zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych,

- 2) instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych,
- 3) innych wytycznych i zasad dotyczących bezpieczeństwa danych i ich przetwarzania.

II. ZASADY UDOSTĘPNIANIA DANYCH OSOBOWYCH

§ 9

1. Szkoła udostępnia dane na miejscu wyłącznie osobom upoważnionym.
2. Upoważnienie może wynikać w szczególności z:
 - 1) pisemnego zakresu czynności, obowiązków wykonywanych na danym stanowisku pracy,
 - 2) z odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.
3. Szkoła dopuszcza do przetwarzania danych w systemie informatycznym, tradycyjnym na mocy pisemnych upoważnień nadanych przez dyrektora lub inną osobę wskazaną przez dyrektora.
4. Upoważnienie wygasa w związku z ustaniem zatrudnienia lub w przypadku pozbawienia upoważnienia w związku z łamaniem ustawy o ochronie danych.
5. Szkoła zapewnia dostęp do przetwarzanych danych osobom, które powierzyły jej swoje dane.

§ 10

1. Osoby niezatrudnione przy przetwarzaniu danych osobowych określonego zasobu, w tym osoby, które dane udostępniły, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych mogą mieć do nich wgląd wyłącznie w obecności upoważnionego pracownika szkoły.
2. Zasada ta obowiązuje także w przypadku korzystania przez związki zawodowe z uprawnień przysługujących im na mocy odrębnych przepisów (k.p., ustawa o związkach zawodowych).
3. Dostęp do danych osobowych i ich przetwarzanie bez upoważnienia dyrektora lub osoby przez niego upoważnionej może mieć nastąpić wyłącznie w przypadku działań osób lub organów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonych zasobów.

4. Dostęp do danych osobowych mogą mieć: Najwyższa Izba Kontroli, Generalny Inspektor Ochrony Danych Osobowych, Zakład Ubezpieczeń Społecznych, Policja, organy skarbowe, Państwowa Inspekcja Pracy, Wojskowe Służby Informacyjne, Agencja Bezpieczeństwa Wewnętrznego, sądy powszechne i inne upoważnione przez przepisy prawa podmioty i organy, na mocy nadanych im uprawnień – po ich okazaniu.

III. PRACOWNICY PRZETWARZAJĄCY DANE

§ 11

1. Zaznajomienie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w szkole może odbywać się poprzez:
 - 1) szkolenia wewnętrzne na terenie szkoły,
 - 2) szkolenie zewnętrzne,
 - 3) instruktaż stanowiskowy,
 - 4) udostępnienie procedury i in. przepisów w tym zakresie.
2. Osoby upoważnione do przetwarzania danych osobowych są zapoznane z zakresem informacji objętych tajemnicą, a także o obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia stosowanych w szkole.

§ 12

Naruszenie zasad bezpiecznego i zgodnego z prawem ich przetwarzania przez pracowników upoważnionych do dostępu, traktowane będzie jako ciężkie naruszenie podstawowych obowiązków pracowniczych ze wszystkimi konsekwencjami, włącznie z rozwiązaniem stosunku pracy.

§ 13

Osoby, których dane są przetwarzane w związku z realizacją celów statutowych szkoły, uzyskują informacje o przysługujących im prawach nadanych ustawą o ochronie danych osobowych.

IV. OBSZAR SZKOŁY, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

§ 14

1. Szkoła wyznacza pomieszczenia i części pomieszczeń, tworzące obszar, w którym przetwarzane są dane.
2. Jeśli w pomieszczeniu, w którym przetwarzane są dane osobowe znajduje się część ogólnodostępna, część, w której są przetwarzane dane, powinna być wyraźnie oddzielona od ogólnodostępnej.
3. Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe, może być poprzez montaż barierek, lad lub odpowiednie ustawienie mebli biurowych uniemożliwiające lub ograniczające dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.
4. Komputery, w których odbywa się praca w związku z przetwarzaniem lub gromadzeniem danych, powinny być ustawiane w sposób uniemożliwiający dostęp do danych.
5. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, określa zarządzenie dyrektora szkoły.
6. W pomieszczeniach i częściach pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, mogą przebywać wyłącznie osoby upoważnione do dostępu i przetwarzania danych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem ich przetwarzania.

§ 15

1. Całkowite opuszczenie (przez pracownika upoważnionego do przetwarzania danych) pomieszczenia, w którym przetwarzane są dane osobowe, może nastąpić po odpowiednim zabezpieczeniu tych danych.
2. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez jego zabezpieczenia oraz znajdujących się w nim zbiorów danych jest niedopuszczalne i będzie traktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

§ 16

1. Dostęp do budynków i pomieszczeń szkoły, w których przetwarzane są dane osobowe podlega kontroli.
2. Kontrola dostępu polegać może na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń.
W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia oraz godzinę pobrania lub zdania klucza.
3. Klucze do pomieszczeń, w których przetwarzane są dane osobowe mogą być wydawane wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom w związku z wykonywaną przez nich pracą.
4. Szkoła realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, może wprowadzać inne formy monitorowania dostępu do miejsc przetwarzania danych osobowych.

V. ZBIORY DANYCH OSOBOWYCH

§ 17

1. Szkoła sprawuje nadzór nad rodzajami oraz zawartością zbiorów danych osobowych tworzonych na jego obszarze. Wykaz zbiorów stanowi odrębny dokument.

§ 18

Szkoła realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, zapewnia – zgodnie z przepisami – ochronę zbiorom danych osobowych sporządzanych doraźnie, ze względów technicznych, szkoleniowych lub w związku z procesem dydaktycznym i wychowawczo-opiekuńczym realizowanym przez szkołę, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji.

§ 19

Szkoła zabrania gromadzenia i tworzenia zbiorów danych osobowych innych niż niezbędne dla realizacji celów statutowych.

VI. USTALENIA KOŃCOWE

§ 20

1. Procedura obowiązuje wszystkich pracowników szkoły, w szczególności tych, którzy tworzą, gromadzą lub w jakikolwiek sposób wykorzystują dane osobowe.
2. Procedura wchodzi w życie z dniem 29.12.2014 r.

.....
(podpis i pieczęć dyrektora)