POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH

W GMINNYM ZESPOLE OBSŁUGI PLACÓWEK OŚWIATOWYCH

W ŚWIERKLANACH

Rozdział I
Postanowienia wstępne.

§ 1

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 – jednolity tekst), oraz § 3 ust. 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 (Dz. U. z 2004 r. Nr 100, poz. 1024 z późn. zm.) ,
ustanawia się Politykę bezpieczeństwa przetwarzania danych osobowych w Gminnym Zespole Obsługi Placówek Oświatowych w Świerklanach, zwaną dalej Polityką bezpieczeństwa.

§ 2

Ilekroć w niniejszym dokumencie jest mowa o :

1) Zespole lub Jednostce - należy przez to rozumieć Gminny Zespół Obsługi Placówek Oświatowych w Świerklanach,

2) ustawie - należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182 – jednolity tekst),

3) rozporządzeniu – należy przez to rozumieć 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 z późn. zm.).

Rozdział II

Zasady przetwarzania i ochrony danych osobowych.

§ 3

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Gminnym Zespole Obsługi Placówek Oświatowych w Świerklanach, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane do zapewnienia poufności, integralności, i rozliczalności przetwarzanych danych osobowych.

2. Polityka Bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych osobowych przetwarzanych zarówno tradycyjnie, jak i w systemach informatycznych. Jej celem jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.

§ 4

1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, zwany dalej „obszarem przetwarzania" - określa **załącznik nr 1** do Polityki Bezpieczeństwa.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik nr 2** do Polityki Bezpieczeństwa.
3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami - określa **załącznik nr 3** do Polityki Bezpieczeństwa.

§ 5

Osoby, które przetwarzają w Zespole dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora Danych Osobowych (wzór upoważnienia - **załącznik nr 4**) oraz podpisać oświadczenie o zachowaniu poufności tych danych (wzór oświadczenia - **załącznik nr 5)**.

§ 6

Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych w systemie informatycznym jednostki posiada swój identyfikator oraz hasło pozwalające na zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe.
Techniczne wymagania, jakie musi spełniać hasło, określone zostały w Instrukcji Zarządzania Systemem Informatycznym w Gminnym Zespole Obsługi Placówek Oświatowych w Świerklanach.

§ 7

W przypadku konieczności dostępu do obszaru przetwarzania danych, osób nie posiadających upoważnienia, które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują one oświadczenie o zachowaniu poufności danych osobowych.

§ 8

Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych, zgodnie z art. 31 ustawy.

§ 9

Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności pisemny wniosek podmiotu uprawnionego.

§ 10

Dokumenty zawierające dane osobowe w formie papierowej, przechowywane są w obszarze przetwarzania danych w szafach zamykanych na klucz. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce dokumentów. Po okresie przydatności dokumentów zawierających dane osobowe do bieżącego wykorzystania, są one przechowywane w zakładowej składnicy akt.

Rozdział III

Organizacja przetwarzania danych osobowych. Zadania osób odpowiedzialnych.

§ 11

1. Nadzór nad przetwarzaniem danych osobowych w Zespole sprawuje Administrator Danych Osobowych (ADO) - kierownik jednostki.
2. Administrator Danych Osobowych, zgodnie z art. 36a ust.1 ustawy, może powołać administratora bezpieczeństwa informacji i powierzyć mu zadania w zakresie zapewnienia przestrzegania przepisów o ochronie danych osobowych w Zespole.
3. Administrator Danych Osobowych może wyznaczyć Administratora Systemu Informatycznego (ASI), który jest odpowiedzialny za przetwarzanie danych osobowych w systemie informatycznym.

§ 12

1. Administrator danych osobowych realizuje obowiązki w zakresie ochrony danych osobowych określone w ustawie. Odpowiada za legalność przetwarzania danych oraz za zapewnienie odpowiednich warunków technicznych i organizacyjnych, decydujących o właściwej ochronie danych osobowych, a w szczególności :

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem zmian w obowiązującym prawie,
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi obowiązków tej osoby,
3) może powołać Administratora bezpieczeństwa informacji (ABI) oraz określa zakres jego zadań i czynności;
4) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator bezpieczeństwa informacji (ABI) realizuje zadania określone w art. 36a ust.2 ustawy, oraz wykonuje inne obowiązki powierzone przez Administratora danych.

3. Administrator systemu informatycznego (ASI) realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora danych osobowych, a w szczególności :

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
3) na wniosek ADO przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
5) wyrejestrowuje użytkowników na polecenie ADO,
6) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ADO o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
7) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
8) wykonuje bieżące czynności serwisowe sieci, sprzętu i oprogramowania jednostki,
9) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
10) wykonuje kopie zapasowe, sprawuje nadzór nad ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
11) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów,

innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

§ 13

Osoba upoważniona do przetwarzania danych ma obowiązek :

1) przetwarzać dane osobowe zgodnie z obowiązującymi przepisami, w szczególności z ustawą i rozporządzeniem oraz ustalonymi procedurami wewnętrznymi,
2) przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków,
3) nie udostępniać danych oraz uniemożliwiać dostęp do nich osobom nieupoważnionym,
4) zabezpieczać dane przed zniszczeniem.

§ 14

Szczegółowe zasady przetwarzania danych osobowych w systemie informatycznym określone zostały w Instrukcji Zarządzania Systemem Informatycznym.

Rozdział IV
Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych).

§ 15

1. Zachowanie poufności.

1. Administrator danych przeprowadza nabór na wolne stanowiska w drodze konkursu. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.

2. Ryzyko utraty bezpieczeństwa danych ze strony pracowników Zespołu jest ponadto minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

3. Ryzyko utraty bezpieczeństwa danych przetwarzanych w Zespole pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci) jest minimalizowane przez zobowiązanie ich do zachowania tajemnicy przez podpisanie pisemnych oświadczeń lub podpisanie umów powierzenia przetwarzania danych osobowych wyspecjalizowanej jednostce zewnętrznej.

2. Strefy bezpieczeństwa.

W siedzibie Zespołu znajdują się cztery pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych, w których dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli.
Strefa ta obejmuje pomieszczenia biurowe znajdujące się na pierwszym piętrze budynku : pokój nr 1 - „Płace i kadry”, pokój nr 2 - „Księgowość”, pokój nr 3 - „Kierownik”, oraz pomieszczenie na parterze pokój nr 4 - „Zakładowa składnica akt”.
W pomieszczeniach biurowych nr 1 - 3 mogą przebywać wyłącznie pracownicy Zespołu, a inne osoby upoważnione tylko w obecności tych pracowników. Osoby postronne mają

dostęp do pomieszczeń w godzinach pracy jednostki, w obecności pracownika Zespołu upoważnionego do przetwarzania danych osobowych.
Do pomieszczenia nr 4 mają dostęp tylko pracownicy jednostki oraz osoba wykonująca prace archiwizacyjne na podstawie odrębnych przepisów oraz wewnętrznych ustaleń z kierownikiem jednostki.

3. Zabezpieczenie sprzętu.

Wszystkie urządzenia systemu informatycznego administratora danych są zasilane za pośrednictwem zasilaczy awaryjnych (UPS). Pracownicy Zespołu – użytkownicy sprzętu komputerowego zostali poinformowani jak postępować, aby zapewnić prawidłową eksploatację systemu informatycznego, a zwłaszcza:

- ochronę nośników przenośnych – w tym także nośników danych, na których przechowywane są kopie zapasowe,
- prawidłową lokalizację komputera.

Bieżąca konserwacja sprzętu wykorzystywanego przez administratora danych do przetwarzania danych prowadzona jest tylko przez jedną firmę zewnętrzną.
Konserwacje i naprawy wykonywane są w siedzibie administratora danych pod nadzorem ASI lub wyznaczonego przez ADO pracownika Zespołu..
Administrator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych.
Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych. Jeżeli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora, uszkodzone urządzenia mogą być przekazywane do utylizacji właściwym podmiotom.

4. Zabezpieczenia we własnym zakresie.

Każda osoba upoważniona do przetwarzania danych jest zobowiązana do przestrzegania następujących zasad :

1) ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;

2) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w miejscach ogólnodostępnych oraz w samochodach;

3) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);

4) pilnego strzeżenia akt, dyskietek, pamięci przenośnych i komputerów przenośnych;

5) kasowania, po wykorzystaniu, danych na dyskach przenośnych;

6) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie, na papierze lub innym nośniku;

7) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń Administratora Systemu Informatycznego;

8) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;

9) kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;

10) nie wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;

11) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;

12) kończenia pracy na stacji roboczej po prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;

13) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

14) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;

15) zachowania tajemnicy danych, w tym także wobec najbliższych;

16) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy.

5. Postępowanie z nośnikami i ich bezpieczeństwo.

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1) Dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone.

2) Uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników.

3) Zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;

4) Po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę Administratora danych.

6. Udostępnianie danych osobowych.

1) Udostępnianie danych osobowych na podstawie ustawy.

Udostępnianie danych osobowych odbiorcom danych może nastąpić wyłącznie w przypadkach określonych ustawą, po złożeniu wypełnionego wniosku, którego wzór został

ustalony na podstawie załącznika nr 1 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 3 czerwca 1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych[1]. Wzór wniosku stanowi **załącznik nr 6** do Polityki bezpieczeństwa.

2) Udostępnianie danych osobowych na podstawie przepisów szczególnych.

a) Udostępnianie informacji Policji.

Udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji.
Wniosek ten, zgodnie z §25 ust. 2 rozporządzenia rozporządzenie Ministra Spraw Wewnętrznych z 31 grudnia 2012 r. w sprawie przetwarzania informacji przez Policję (Dz. U z 2013 r., poz. 8), powinien mieć formę pisemną i zawierać następujące dane :

- oznaczenie sprawy,
- określenie zbioru danych, z którego informacje maja zostać udostępnione,
- wskazanie informacji podlegających udostępnieniu,
- wskazanie wnioskodawcy,
- wskazanie podstawy prawnej udostepnienia informacji,
- oznaczenie formy przekazania lub udostępnienia informacji,
- imię, nazwisko, stopień służbowy lub zajmowane stanowisko osoby upoważnionej do pobrania informacji lub zapoznania się z ich treścią.

Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania.

Osoba udostępniająca dane osobowe jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji.

Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie (potwierdzenie). Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.

Jeśli policjant pouczył osobę udostępniającą informacje o konieczności zachowania w tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępnienia informacji.

b) Udostępnianie danych osobowych innym służbom.

Udostępnianie danych osobowych innym służbom może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną. Udostępnianie danych osobowych na podstawie ustnego wniosku może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania w celu albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.

[1] Dz. U nr 80, poz. 522 ze zm. Rozporządzenie już nie obowiązuje, lecz Generalny Inspektor przyjmuje, że jego treść odpowiada wymaganiom ustanowionym przez ustawę i dlatego może być nadal stosowane.

Rozdział V
Postanowienia końcowe

§ 16

Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z art. 49 - 54a ustawy o ochronie danych osobowych.

§ 17

W sprawach nieuregulowanych niniejszym dokumentem, mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j. t. - Dz.U. z 2014 r., poz. 1182 z późn.zm.) oraz rozporządzenia wydanego na podstawie art. 39a ww. ustawy.

……..……
podpis Administratora Danych Osobowych

SPIS ZAŁĄCZNIKÓW :

Załącznik nr 1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

Załącznik nr 2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

Załącznik nr 3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

Załącznik nr 4. Upoważnienie do przetwarzania danych osobowych.

Załącznik nr 5. Oświadczenie o zachowaniu poufności danych osobowych.

Załącznik nr 6. Wniosek o udostępnienie danych osobowych.