POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W PUBLICZNYM PRZEDSZKOLU NR 23 W JASTRZĘBIU-ZDROJU

ROZDZIAŁ I
Postanowienia ogólne

§ 1

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Publicznym Przedszkolu Nr 23 w Jastrzębiu-Zdroju zwana dalej „Polityką bezpieczeństwa" ,określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:
   1) tradycyjnych, w szczególności kartotekach, księgach, skorowidzach, aktach osobowych, wykazach, w zbiorach ewidencyjnych;
   2) w systemach informatycznych - ewidencje statystyczne, plany organizacyjne.

2. Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1) ***ustawie*** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z poźn. zm.);

2) ***administrator bezpieczeństwa informatycznego (ABI)*** –rozumie się Dyrektora Publicznego Przedszkola Nr 23 w Jastrzębiu-Zdroju.

3) ***lokalny administrator danych osobowych*** – rozumie się pracowników administracyjnych przedszkola, wychowawców, nauczycieli;

4) ***administrator sieci*** –rozumie się osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych;

5) ***nośniki danych osobowych*** – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi;

6) ***osoba upoważniona (użytkownik)*** –osoba posiadająca upoważnienie wydane przez dyrektora.

7) ***dane osobowe*** - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

8) ***przetwarzanie danych*** - rozumie się przez to 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;

9) ***zbiór danych*** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;

10) ***system informatyczny*** -zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

11) ***identyfikator użytkownika (login)*** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie

obsługi systemu ręcznego i informatycznego używanego do gromadzenia i przetwarzania danych osobowych (*załącznik nr 2*)

2. Pracownicy wymienieni w pkt 1 zbierają i przetwarzają dane osobowe wyłącznie do realizacji celów wymienionych w rozdziale I.
3. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:
   - imię i nazwisko osoby upoważnionej,
   - datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
4. Upoważnienia, o których mowa w ust. 1, są imienne i udzielane w formie pisemnej na czas określony lub na czas nieokreślony – do odwołania udzielonego upoważnienia.
5. Każde upoważnienie jest rejestrowane w rejestrze upoważnień oraz przechowywane w aktach osobowych pracownika.
6. Osoby mające upoważnienie do ręcznego i informatycznego przetwarzania danych osobowych zobowiązane są do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.
7. Osoby, o których mowa w pkt 1, mające upoważnienie do przetwarzania danych w systemie informatycznym zobowiązane są do bezwzględnego przestrzegania instrukcji zawartej w rozdziale VIII.
8. Osoby, o których mowa w pkt 1, mające dostęp do danych osobowych, obowiązane są do zachowania ich w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia.

ROZDZIAŁ VIII

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

§ 12

1. Dyrektor przedszkola jest obowiązany pełnić rolę Administratora Bezpieczeństwa Informatycznego (ABI) w placówce.
2. ABI jest odpowiedzialny za właściwy nadzór nad funkcjonowaniem systemu ochrony danych osobowych.
3. Miejscami przetwarzania danych osobowych z użyciem sprzętu komputerowego są:
   - Sekretariat-gabinet intendenta
   - gabinet dyrektora,
4. Przebywanie osób nieuprawnionych w miejscach, o którym mowa w pkt 3 jest dopuszczalne tylko w obecności osób zatrudnionych przy przetwarzaniu danych i za zgodą ABI.
5. Procedura rozpoczęcia i zakończenia pracy.

   Użytkownik systemu:
   - uruchomia komputer odpowiednim hasłem,
   - ustawia ekrany monitorów na stanowiskach, na których przetwarzane są dane osobowe, tak, aby osoby nieupoważnione nie miały dostępu do informacji na nich wyświetlanych,
   - upewnia się, że osoby nieupoważnione nie mają możliwości wglądu do danych, w razie przerwania pracy włącza wygaszacz ekranu,
   - upewnia się, czy dane zostały zarejestrowane, aby uniknąć utraty danych z powodu awarii,
   - nie udostępnia pomieszczeń, w których są przetwarzane dane, osobom postronnym podczas nieobecności osób zatrudnionych przy informatycznym przetwarzaniu danych osobowych,
   - kończy pracę związaną z przetwarzaniem danych osobowych według wszystkich reguł bezpieczeństwa informacji.
6. Kopie informatyczne, wydruki wykonuje się w miarę potrzeb i przechowuje w sposób określony przepisami.
7. Kopie awaryjne przechowuje się zgodnie z prawem i okresowo sprawdza pod kątem przydatności.
8. Nośniki danych oraz wydruki, które nie są przeznaczone do udostępniania, przechowuje się w zamykanej szafie, do której dostęp mają tylko osoby uprawnione.
9. W razie stwierdzenia naruszenia systemów informatycznych należy bezzwłocznie poinformować ABI.
10. ABI sprawdza stan urządzeń, zawartość zbiorów danych osobowych i wielkość ich naruszenia.
11. Dane uzupełnia się na podstawie kopii awaryjnych.

informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopi zapasowych, prace na danych osobowych w celach prywatnych itp.);
- nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych, znajdujących się na dyskach, płytach CD, kartach pamięci oraz wydrukach komputerowych w formie niezabezpieczonej (otwarte szafy, biurka, regały, archiwum).

ROZDZIAŁ V
Przekazanie informacji osobom, których dane będą zbierane

§ 8

1. Obowiązek informowania, a także uzyskania oświadczeń woli traktowany jest łącznie w stosunku do grup, których dane placówka zbiera i przetwarza.
2. W przypadku pracowników obowiązek, o którym mowa w pkt.1 uważa się za spełniony po podpisaniu druku stanowiącego ***załącznik nr 1.***
3. W przypadku dzieci i rodziców obowiązek, o którym mowa w pkt. 1 uważa się za spełniony po podpisaniu przez rodziców (prawnych opiekunów) umowy.

ROZDZIAŁ VI
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

§ 9

1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:
   1) wszystkie pomieszczenia, w których przetwarzane są dane osobowe zamykane są na klucz, w przypadku opuszczenia przez ostatnia osobę upoważnioną do przetwarzania danych osobowych – także w godzinach pracy;
   2) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash (pen drajw) płyty CD, DVD, dyskietki) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych.
   3) nieaktualne lub błędne wydruki zawierające dane osobowe są niszczone.
   4) budynek, w którym są przetwarzane dane chroniony jest całodobowo przez pracowników ochrony Almar.

§ 10

1. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:
   1) ochrona przed utratą danych poprzez cykliczne wykonywanie kopi zapasowych;
   3) zapewnienie właściwej temperatury i wilgotności w pomieszczeniach;
   4) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w dostępnej odległości gaśnic;

2. Organizację ochrony danych osobowych realizuje się poprzez:
   1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do pracy;
   2) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych i programów;
   3) kontrolowanie pomieszczeń budynku;
   4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

ROZDZIAŁ VII
Obowiązki pracowników w zakresie ochrony danych osobowych

§ 11

1. Pracownicy zatrudnieni w przedszkolu (nauczyciele, intendent) otrzymują upoważnienie do

- Zbiór 21 – Dokumenty archiwalne;
- Zbiór 22 – Teczki awansu zawodowego;
- Zbiór 23 – Arkusz organizacyjny placówki;

§ 5

1.Zbiory danych osobowych wymienione w § 4 ust.1 podlegają przetwarzaniu w sposób tradycyjny lub informatyczny.

2. Wszystkich pracowników, którzy gromadzą i przetwarzają dane osobowe zobowiązuje się do bezwzględnego przestrzegania przepisów ustawy przywołanej we wstępie oraz niniejszej instrukcji.

ROZDZIAŁ III
Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych.

§ 6

1 .Dane osobowe gromadzone i przetwarzane są w budynku przedszkolnym, mieszczącym się w Jastrzębiu-Zdroju ulica 1-go Maja 3a.

2. Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są :

1) sekretariat przedszkolny-gabinet intendenta
2) gabinet dyrektora
3) składnica – archiwum szkolne.

ROZDZIAŁ IV
Opis zdarzeń naruszających ochronę danych osobowych

§ 7

1. Rodzaje zagrożeń naruszających ochronę danych osobowych:

a). Zagrożenia losowe:

- zewnętrzne np. klęski żywiołowe, przerwy w zasilaniu – ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu: ciągłość zostaje naruszona , jednak nie dochodzi do naruszenia danych osobowych;
- wewnętrzne np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania w wyniku ich wystąpienia może dojść do zniszczenia danych, może nastąpić zakłócenie ciągłości pracy systemu i naruszenia poufności danych.

b) Zagrożenia zamierzone (świadome i celowe naruszenia poufności danych) – w wyniku ich wystąpienia zazwyczaj nie występuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. W ramach tej kategorii zagrożeń wystąpić mogą:

- nieuprawniony dostęp do systemu z zewnątrz;
- nieuprawniony dostęp do systemu z wewnątrz;
- nieuprawnione przekazanie danych;
- bezpośrednie zagrożenie materialnych składników np. kradzież, zniszczenie.

2. Okoliczności zakwalifikowane, jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

- sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby systemu np. wybuch gazu, pożar, zalanie pomieszczeń, uszkodzenia wskutek prowadzonych prac remontowych;
- niewłaściwe parametry środowiska np. nadmierna wilgotność, temperatura, wstrząsy, oddziaływania pola elektromagnetycznego, przeciążenia napięcia;
- awarie sprzętu lub oprogramowania, które są celowym działaniem na potrzeby naruszenia ochrony danych osobowych;
- pogorszenie, jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie;
- rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa

informatycznym;

12) ***hasło*** ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

13) ***uwierzytelnianie*** —rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
14) ***poufności danych*** — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§ 2

1.Dyrektor Przedszkola realizując politykę bezpieczeństwa dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia , aby dane te były:

1) przetwarzane zgodnie z prawem;
2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane przetwarzaniu niezgodnemu z tymi celami;
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą.

3.Dyrektor Przedszkola dąży do systematycznego unowocześniania stosowanych na terenie placówki informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnianiem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą , uszkodzeniem lub zniszczeniem.

§ 3

1. Cele, dla których Publiczne Przedszkole Nr 23 w Jastrzębiu-Zdroju zbiera dane osobowe, to:

1) Rejestrowanie przebiegu zatrudnienia i wynagradzania pracowników.
2) Realizacja zadań dydaktycznych i wychowawczo-opiekuńczych.
3) Rekrutacja do przedszkola.
4) Gromadzenie ofert pracy.

ROZDZIAŁ II
Wykaz zbiorów danych osobowych w Publicznym Przedszkolu Nr 23

§ 4

1 . Dane osobowe gromadzone są w zbiorach:

- Zbiór 1 –Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych;
- Zbiór 2 –Kontrola wewnętrzna- wyniki, opracowania, protokóły, notatki,;
- Zbiór 3 –Akta osobowe pracowników;
- Zbiór 4 –Dokumentacja dotycząca polityki kadrowej;
- Zbiór 5 –Notatki służbowe oraz postępowanie dyscyplinarne;
- Zbiór 6 – Zbiory informacji o pracownikach
- Zbiór 7 – Skierowania na badania okresowe, specjalistyczne;
- Zbiór 8 –Ewidencja zasobów szkoły –SIO;
- Zbiór 9 –Ewidencja urlopów, karty czasu pracy;
- Zbiór 10 – Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej;
- Zbiór 11 – Rejestr delegacji służbowych;
- Zbiór 12 – Karty zgłoszeń dzieci , umowy;
- Zbiór 13 – Dzienniki zajęć obowiązkowych i dodatkowych;
- Zbiór 14 – Zaświadczenia z PPP i inne orzeczenia i opinie;
- Zbiór 15 –Deklaracje uczęszczania na religię,
- Zbiór 16 – Rejestr zaświadczeń wydanych pracownikom przedszkola;
- Zbiór 17 – Rejestr wypadków, ewidencja podejrzeń o chorobę zawodową, itp;
- Zbiór 18 – Księga druków ścisłego zarachowania;
- Zbiór 19 – Zbiór upoważnień
- Zbiór 20 – Protokóły rad pedagogicznych , księga uchwał;