PRZEDSZKOLE "MIŚ"
W PNIEWACH
ul. Dworcowa 23, 62-045 Pniewy
tel. 61 29 11 216
NIP 7871967080 REGON 631578839

Polityka Ochrony Danych Osobowych

w Przedszkolu „Miś" w Pniewach

1. Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Przedszkole „Miś" w Pniewach w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO) oraz Ustawy o ochronie danych osobowych z dnia 10 maja 2018 roku (UODO).
Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z RODO i UODO.

2. Definicje

Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Administrator (A) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

Przedstawiciel - oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;
Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

IOD – Inspektor Ochrony Danych;

ASI – Administrator Systemu Informatycznego, osoba wyznaczona, powoła przez Administratora do wykonywania czynności administracyjnych dotyczących systemu IT;

Przetwarzanie danych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Aktywa - środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych;

Naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

Incydent – pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działania i zagrażają bezpieczeństwu informacji;

Zagrożenie – potencjalna przyczyna niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;

Podatność – uchybienie, luka, błąd, słaby punkt, którego istnienie powoduje, że zagrożenie jest mniej lub bardziej realne; „dzięki" podatności może dojść do realizacji, wystąpienia zagrożenia; słabość zasobu lub zabezpieczenia systemu, która może zostać wykorzystana przez zagrożenie;

Skutki - rezultaty incydentu, straty w wypadku wystąpienia zagrożenia;

Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów;

3. Dane osobowe, zasoby, zgodność z prawem, upoważnienia

3.1 Inwentaryzacja zasobów

1. Przetwarzane dane osobowe zostały zinwentaryzowane w *Wykazie zbiorów danych osobowych* (Załącznik nr 1).
2. Wykaz obejmuje wszystkie zbiory danych osobowych przetwarzane przez Administratora, także ze stwierdzonym potencjalnym ryzykiem naruszenia praw i wolności osób fizycznych z podaniem cech zbiorów istotnych dla procesu przetwarzania.
3. Przetwarzane zbiory zostały opisane w sposób umożliwiający przeprowadzenie analizy ryzyka z uwzględnieniem posiadanych aktywów zinwentaryzowanych w *Rejestrze, liście aktywów zasobów* (Załącznik nr 2), wdrożonych i zastosowanych zabezpieczeń zinwentaryzowanych w *Rejestrze, liście zabezpieczeń* (Załącznik nr 3) oraz określonych, oszacowanych zagrożeniach zinwentaryzowanych w *Rejestrze, liście zagrożeń i podatności* (Załącznik nr 4)
4. Dodatkowo dla wspomagania procesów inwentaryzacji posiadanych zasobów ASI może prowadzić *Karty zasobów* (Załącznik nr 5).

3.2 Zgodność przetwarzania z prawem

1. Administrator przeanalizował, sprawdził i zapewnia:
   - dane osobowe są legalnie przetwarzane zgodnie z art. 6, 9 RODO;
   - dane osobowe są adekwatne w związku z celem przetwarzania;
   - dane są przetwarzane przez konkretny, określony, dopuszczony czas
   - wobec osób, których dane są przetwarzane dopełniono obowiązku informacyjnego wraz ze wskazaniem im praw zgodnie z art. 12, 13, 14 RODO;
   - zapewniono informację o żądaniach podmiotu danych w prowadzonym *Rejestrze realizacji żądania podmiotu danych* (Załącznik nr 6)
   -zapewniono ochronę danych w przypadku dokonania powierzenia przetwarzania danych w postaci zawarcia stosownych umów powierzenia z podmiotami przetwarzającymi i wydania upoważnień powierzenia dla osób, którym powierzono przetwarzanie danych osobowych zgodnie z art. 28 RODO.
   -zapewniono informację o powierzeniach przetwarzania danych osobowych w prowadzonym *Rejestrze powierzeń danych osobowych* (Załącznik nr 7)
   -zapewniono informacje o udostępnieniach danych osobowych w prowadzonej *Ewidencji udostępnienia danych osobowych* (Załącznik nr 8).
2. Potwierdzenie przetwarzania zgodnie z prawem danych osobowych znajduje się w *Wykazie zbiorów danych osobowych* (Załącznik nr 1) w polu *„Cel przetwarzania, podstawa prawna".*
3. Klauzule informacyjne są opracowywane i aktualizowane według potrzeb, umieszczono je w *Rejestrze, wykazie klauzul informacyjnych i zgód* (Załącznik nr 9)

3.3 Upoważnienia.

1. Administrator odpowiada za proces nadawania, anulowania upoważnień do przetwarzania danych osobowych w zbiorach danych osobowych, a także generowanie dostępu do systemów informatycznych przeznaczonych do przetwarzania danych osobowych.

2. Każdy użytkownik musi przetwarzać dane osobowe wyłącznie na polecenie administratora lub na podstawie odpowiedniego przepisu prawa.
3. Upoważnienia do przetwarzania danych osobowych nadawane są do przetwarzanych zbiorów danych osobowych wyłącznie na wniosek przełożonych według wzoru *Upoważnienie do przetwarzania danych osobowych* (Załącznik nr 10) w związku i zgodnie z obowiązkami służbowymi.
4. Dodatkowa dla wspomagania procesu wydawania upoważnień ASI może prowadzić *Karty konta indywidualnego* (Załącznik nr 11).
5. Dopuszcza się wydawanie upoważnień w formie udokumentowanych poleceń, umów powierzenia, umów realizacji czynności związanych z potencjalnym dostępem lub dostępem do danych osobowych, dostępem do obszarów przetwarzania danych osobowych.
6. Administrator, IDO prowadzi ewidencję upoważnień w celu sprawowania kontroli nad prawidłowością procesu dostępu do danych osobowych zgodnie z *Rejestrem upoważnień* (Załącznik nr 12).

4. Procedury przeprowadzenia analizy ryzyka i oceny skutków przetwarzania

4.1 Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia przetwarzanych danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

4.2 Założono, że analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów danych osobowych charakteryzujących się podobieństwem celów i sposobów przetwarzania, zgodnością zasobów użytych do procesu przetwarzania.

4.3 Ocenę skutków przetwarzania danych osobowych zgodnie z art. 35 RODO wykonujemy przez realizację czynności:
- opis planowanych operacji i celów przetwarzania, opis w *Wykazie zbiorów danych osobowych* (Załącznik nr 1);
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów, opis w *Wykazie zbiorów danych osobowych* (Załącznik nr 1);
- wyznaczenie i ocenę ryzyka przetwarzania zgodnie z *Procedurą analizy ryzyka* (Załącznik nr 13);
- zaplanowaniu, przyjęciu i wdrożeniu środków w celu ograniczenia, wyeliminowania ryzyka, przedstawionego w postaci planu postępowania z ryzykiem.

4.4 Dopuszcza się zastosowanie innych procedur, metod przeprowadzania analizy ryzyka w tym wykorzystywania oprogramowania.

5. Instrukcja postępowania z incydentami naruszenia ochrony danych osobowych

5.1 Instrukcja ma na celu określenie reakcji na wystąpienie incydentu naruszenia ochrony danych osobowych, minimalizację skutków incydentu oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów.

5.2 Każda osoba przetwarzającą dane osobowe lub mająca informacje dotyczące procesu przetwarzania danych osobowych jest zobowiązana do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu naruszenia ochrony danych osobowych bezpośredniego przełożonego, ASI lub IOD. Dla wspomagania tego procesu prowadzony jest *zeszyt zgłoszeń* dostępny w Sekretariacie, siedzibie Administratora.

5.3 Typowe podatności:
-niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
- niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka i ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

5.4 Typowe incydenty naruszeń ochrony danych osobowych:
- zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
- zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
- umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych, kradzież sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

5.5 W przypadku stwierdzenia wystąpienia incydentu naruszenia ochrony danych osobowych Administrator, IOD prowadzi postępowanie wyjaśniające w toku, którego:
- ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
- inicjuje ewentualne działania dyscyplinarne;
- ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
- działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;
- rekomenduje działania prewencyjne, zapobiegawcze zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia

5.6 Administrator, IOD dokumentuje powyższe czynności incydentu naruszenia ochrony danych w *Rejestrze naruszeń ochrony danych osobowych* (Załącznik nr 14) i sporządza stosowny *Raport z naruszenia ochrony danych osobowych* (Załącznik nr 15)

5.7 Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

5.8 W przypadku incydentu naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych Administrator, IOD bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je organowi nadzorczemu zgodnie z *Zgłoszeniem z naruszenia ochrony danych osobowych* (Załącznik nr 16).

6. Regulamin ochrony danych osobowych, szkolenia.

6.1 Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania danych osobowych.

6.2 Po zapoznaniu się z zasadami ochrony danych osobowych zawartymi w *Regulaminie ochrony danych osobowych* (Załącznik nr 17) osoby zobowiązane są do podpisania *Oświadczenia poufności* (Załącznik nr 18).

6.3 Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO i UODO.

6.4 Za przeprowadzenie szkolenia odpowiada Administrator, IOD.

6.5 Przeprowadzanie szkoleń dokumentowane jest listą obecności na szkoleniu z podaniem miejsca, daty i danych prowadzącego szkolenie.

6.6 Szkolenie prowadzone są dla nowych pracowników i cyklicznie dla wszystkich pracowników zgodnie z zapotrzebowaniem.

6.7 Szkolenie obejmuje tematykę RODO i UODO oraz przyjęte zasady ochrony danych osobowych określone w niniejszej *Polityce ochrony danych osobowych* oraz w *Regulaminie ochrony danych osobowych* (Załącznik nr 17).

7. Rejestr czynności przetwarzania

7.1 W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Administratora stosujemy *Rejestr czynności przetwarzania danych osobowych* (Załącznik nr 19).

7.2 W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Podmiot przetwarzający stosujemy *Rejestr kategorii czynności przetwarzania danych osobowych* (Załącznik nr 20).

8. Audyty

8.1 Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.W tym celu Administrator stosuje procedurę audytów zgodnie z *Procedurą audytów* (Załącznik nr 21).

9. Procedury awaryjne, kopie

9.1 Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. W tym celu Administrator opracował procedury przywracania, opisane w *Planie ciągłości, kopie* (Załącznik nr 22).

9.2 Opis wykonywania kopii opisano w *Planie ciągłości, kopie* (Załącznik nr 22).

10. Wykaz zabezpieczeń, dokumentacja

10.1 Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych opisane w *Rejestrze, liście zabezpieczeń* (Załącznik nr 3).

10.2 Celem identyfikacji czynności w systemie IT ASI prowadzi *Dziennik administratora systemu IT* (Załącznik nr 23) .

10.3 Celem zapewnienia awaryjnego dostępu do systemu IT sporządzono dokumentację haseł dostępowych do systemu IT zgodnie z *Metryką haseł* (Załącznik nr 24). Metrykę haseł deponuje się w zabezpieczonej, podpisanej kopercie w sejfie lub w szafie pancernej. Dostęp do *Metryki haseł* ma Administrator, ASI i IOD.

10.4 Celem udokumentowania procesu niszczenia, usuwania danych osobowych stosuje w procedurze niszczenia *Protokół zniszczenia nośników danych osobowych* (Załącznik nr 25).

10.5 W wykazie wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne.

10.6 Wykaz jest aktualizowany po każdej analizie ryzyka.

10.7 ASI powinien posiadać i prowadzić na bieżąco dokumentację techniczną zawierającą:

-Projekt sieci logicznej, elektrycznej na planach budowlanych;
-Pomiary statyczne, dynamiczne i elektryczne sieci;
-Schemat, plan logiczny sieci;
-Schemat, plan fizyczny sieci;
-Opis konfiguracji sieci, funkcji, punktów dystrybucji, usług świadczonych na zewnątrz i wewnątrz;
-Ewidencja usług;
-Ewidencję sprzętu komputerowego;
-Ewidencję oprogramowania, licencji;
-Ewidencję zasobów – *karty zasobów (Załącznik nr 5);*
-Ewidencje kopii bezpieczeństwa;
-Ewidencję użytkowników – *karty wyposażenia indywidualnego, karty konta indywidualnego (Załącznik nr 11);*
-Ewidencję kont pocztowych;
-Ewidencję autoryzacji i haseł dostępowych;
-Ewidencję umów z zakresu usług IT;
-*Dziennik administratora systemu IT (Załącznik nr 23).*

10.8 Administrator lub służby organizacyjne Administratora prowadzą według potrzeb *Ewidencję pobrań (Załącznik nr 27), Ewidencję dostępu do pomieszczeń(Załącznik nr 28),* bądź też wdrożyły *„Politykę kluczy" (Załącznik nr 26)*

UWAGA: Dołączono diagramy funkcjonalne dla zobrazowania kluczowych procesów przetwarzania danych osobowych wykorzystywane do zobrazowania wykonywanych czynności

Dyrektor Przedszkola
mgr Katarzyna Kurek-Bryk