POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH

Dla

Niepublicznego Przedszkola "Akademia Małego Odkrywcy" ARTUR STRZELECKI, ROBERT RYBAK
ul. Kazimierza Wielkiego 2A,
41-400 Mysłowice

tel. 531 583 333

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE

§1

1. Celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Niepublicznego Przedszkola "Akademia Małego Odkrywcy" Artur Strzelecki w Mysłowicach, jako Administratora Danych Osobowych, z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych.
2. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem'
3. Niniejsza polityka jest zgodna z obowiązującymi przepisami prawa, oparta o wytyczne zawarte w następujących aktach prawnych:

a) Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2018 r. poz. 1000);
b) Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE [rozporządzenie ogólne o ochronie danych];
c) Rozporządzeniu 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 (U. 2004 nr 100 poz. 1024),

§2.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1) Przedszkole - Niepubliczne Przedszkole "Akademia Małego Odkrywcy" Artur Strzelecki, Robert Rybak w Mysłowicach.
2) Administrator danych osobowych - osoba ustalający cele i sposoby przetwarzania danych osobowych w Niepublicznym Przedszkolu "Akademia Małego Odkrywcy" w Mysłowicach - właściciel przedszkola.
3) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
4) przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych np. gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych,
5) Użytkownik - rozumie się przez to osobę wyznaczoną i upoważnioną przez Administratora danych do przetwarzania danych osobowych, przeszkoloną w zakresie ochrony tych danych.

6) system informatyczny – system przetwarzania danych w Przedszkolu za pomocą sprzętu komputerowego.
7) zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.
8) Zbiór danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

II. DEFINICJA BEZPIECZEŃSTWA

§3.

1. Utrzymanie bezpieczeństwa danych osobowych przetwarzanych przez Przedszkole rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszych Wymagań Bezpieczeństwa.
2. Definicje pojęć w odniesieniu do informacji:
   1) Poufność informacji – rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
   2) Integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
   3) Dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   4) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych i zbiorów papierowych
3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   1) Niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
   2) Niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,

3) Rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES

§4.

1. W systemie informacyjnym Przedszkola przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z obowiązujących przepisów prawa.
2. Informacje te są przetwarzane i przechowywane zarówno w postaci papierowej jak i elektronicznej.

§5.

Wymagania bezpieczeństwa stosuje się do:

1. danych osobowych przetwarzanych w systemie informatycznym,
2. danych osobowych przetwarzanych w systemie papierowym,
3. wszystkich informacji dotyczących danych pracowników, w tym danych osobowych personelu i treści zawieranych umów o pracę,
4. Wszystkich informacji dotyczących danych dzieci i ich rodziców,
5. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
6. rejestru osób dopuszczonych do przetwarzania danych osobowych,
7. zbiorów danych i innych dokumentów zawierających dane osobowe

§6.

1. Zakresy określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do całego systemu informacyjnego w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
2) wszystkich pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy oraz inne osoby mające dostęp do informacji podlegających ochronie.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI

§7.

1. Dokumenty Polityki Bezpieczeństwa ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa składa się z:

1) Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
2) Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w Przedszkolu - załącznik nr 1,
3) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia- załącznik nr 2.
4) Analizy ryzyka.
5) Rejestru przetwarzania danych.

V. DOSTĘP DO INFORMACJI

§8.

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką Bezpieczeństwa danych, Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych obowiązującymi w Przedszkolu.

§9.

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§10.

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, mogą być udostępnione jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

§11.

Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§12.

1. Na wniosek osoby, której dane dotyczą dostarcza się w formie pliku PDF kopię jej danych osobowych oraz udziela się następujących informacji:

1) Cel lub cele przetwarzania danych,
2) kategorię danych osobowych,
3) informację o odbiorcach danych (jeżeli istnieją),
4) planowany okres przechowywania danych,
5) prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych,
6) prawie wniesienia skargi do organu nadzorczego,
7) profilowaniu danych (jeśli dotyczy),
8) o źródle pozyskanych danych – jeżeli dane nie zostały zebrane od osoby której dane dotyczą.

2. Wzory zawierające informacje wypełniające obowiązek informacyjny znajdują się w załączniku nr 6

VI. ZARZĄDZANIE DANYMI OSOBOWYMI

§13.

Za bezpieczeństwo danych osobowych odpowiada administrator danych osobowych wdraża odpowiednie środki techniczne i organizacyjne aby przetwarzanie danych odbywało się zgodnie z prawem, tak aby móc wykazać ten fakt. Środki stosowane w tym celu w razie potrzeby podlegają okresowej kontroli i mogą być uzupełniane.

§14

W umowach zawieranych przez podmiot przetwarzający dane winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnionych przez podmiot przetwarzający dane lub w odrębnych umowach powierzenia przetwarzania danych osobowych.

§15.

Zapoznanie się z dokumentami określonymi w §7 ust.2 pracownicy firmy potwierdzają podpisem na stosownym oświadczeniu (wzór w załączniku nr 5) i przekazują administratorowi danych osobowych.

§16.

Ochrona zasobów danych osobowych jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników.

VII. ZAKRESY OBOWIĄZKÓW I ODPOWIEDZIALNOŚCI

§18.

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik.

§19.

Administrator danych osobowych:

1. odpowiada za realizację przepisów prawa wymienionych w niniejszej Polityce
2. sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
3. identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych.
4. określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe, i innych nośnikach w których przetwarzane są dane osobowe
5. sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,
6. sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
7. przyznaje użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,

8. prowadzi nadzór nad prowadzeniem zbiorów,
9. prowadzi nadzór nad prowadzeniem ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.

§20.

Administrator danych osobowych zobowiązany jest do przestrzegania wszystkich przepisów obowiązującego prawa, w szczególności poprzez:

1. określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych,
2. określenie pomieszczeń w którym przetwarzane są dane osobowe.,
3. zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
4. wdrażanie i nadzorowanie przestrzegania Polityki niniejszej Polityki
5. działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,
6. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązujących przepisów prawa dotyczących ochrony danych,
7. odpowiedzialność za poprawność merytoryczną danych.

§21.

W zakresie systemu informatycznego Administrator danych osobowych odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. konfigurację i administrację oprogramowaniem systemowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
3. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
4. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
5. zarządzanie licencjami, procedurami ich dotyczącymi,
6. prowadzenie profilaktyki antywirusowej.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

§22.

Ze względu na specyfikę przetwarzania danych osobowych, które zawierają dane wrażliwe, oraz ze względu na bezpieczeństwo dzieci wprowadza sie następujące zasady:

1. Rozmowy przeprowadzane pomiędzy personelem, a rodzicami odbywają się jedynie w wyznaczonym pomieszczeniu (gabinet właścicielki Firmy), który zapewnia pełną dyskrecję przeprowadzonej rozmowy.
2. Nie używa się nazwisk dzieci.
3. Niezbędne Informacje umieszczane w korytarzach oraz salach w których odbywają się zajęcia, a które w bezpośredni sposób dotyczą dzieci są chronione poprzez umieszczania na tych dokumentach jedynie imion dzieci. W przypadku powtarzających się imion dodatkowo umieszcza sie pierwszą literę nazwiska. W przypadku gdy imię dziecka i pierwsza litera nazwiska jest taka sama, można umieścić dodatkową cechę dziecka. Określenie takie cechy nie może być dla dziecka obraźliwe czy w inny sposób naruszające jego godność.
4. Zakazuje się upubliczniania na tablicy ogłoszeń żadnych informacji zawierających dane umożliwiające identyfikację dziecka.
5. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach zamykanych na klucz przez wyznaczone do tego celu osoby.
6. Pomieszczenia, w których przetwarzane są dane osobowe, są zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
7. Dokumenty zawierające dane osobowe, których posiadanie jest niezbędne opiekunce dla zapewnienia prawidłowej opieki nad dzieckiem oraz dla kontroli osób odbierających dziecko z przedszkola są przetwarzane w salach zajęciowych. Po zakończeniu zajęć dokumenty te są przenoszone do wyznaczonych zabezpieczonych pomieszczeń w których są przechowywane dane osobowe.
8. Wprowadza się zasadę czystego biurka i pulpitu komputera w przypadku wejścia do pomieszczeń w których są przetwarzane dane osobowe osób nieuprawnionych.
9. W przypadkach kiedy istnieje konieczność przekazania informacji o dziecku rodzicowi czy opiekunowi, której ze względu na swój charakter nie może być przekazana w obecności osób trzecich, a nie można skorzystać z formy opisanej w pkt.1, należy niezwłocznie przekazać taką informację telefonicznie lub za pomocą poczty elektronicznej.

§23.

1. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć za pomocą niszczarki.
2. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych osobowych.

X. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI PRZETWARZANYCH DANYCH

§25.

Stosuje się następujące zabezpieczenia danych osobowych:

1. Zabezpieczenia fizyczne:
   - odrębne pomieszczenia zamykane na klucz,
   - szafy zamykane na klucz
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   - przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   - przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
3. Zabezpieczenia komputera poprzez zastosowania haseł i zamykanie go w pomieszczeniu zamykanym na klucz.
4. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:

1) wykaz pracowników uprawnionych do przetwarzania danych osobowych, znajduje się w załączniku nr 7.
2) przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie
3) w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
4) przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,
5) w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
6) po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

XI. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§27.

Archiwizacja informacji zawierających dane osobowe odbywa w formie elektronicznej oraz papierowej. Nośniki danych przechowywane są w wydzielonym pomieszczeniu - Pomieszczenie w

którym są przechowywane dokumenty archiwalne są zabezpieczone przed dostępem osób nieupoważnionych.

XII. POSTANOWIENIA KOŃCOWE

§28.

1. Administrator Danych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
3. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
4. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.