Polityka ochrony danych osobowych

Administrator: Placówka oświatowa .....

PRYWATNE PRZEDSZKOLE
PIOTRUSIA PANA
I.Lecka-Karnas, B.Tarapacz
ul. Żabiniec 45, 31-215 Kraków
tel. 12 416-37-67

Data przyjęcia: 25.V.2018 r.

I Wprowadzenie

Zgodnie z wymogami *Rozporządzenia 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* (ogólne rozporządzenie o ochronie danych – dalej Rozporządzenie UE) oraz *Ustawy o ochronie danych osobowych* administrator Prywatne Przedszkole „Piotrusia Pana"
(nazwa placówki oświatowej)
zarządza procesem przetwarzania danych osobowych w ramach swojej organizacji, zgodnie z zasadami opartymi na obowiązujących przepisach w zakresie danych osobowych, które zostały zebrane w niniejszej Polityce ochrony danych osobowych.

Polityka ochrony danych osobowych, zwana dalej Polityką, została sporządzona w związku z wymaganiami *Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych – dalej RODO) oraz *Ustawy o ochronie danych osobowych.*

W ramach tego dokumentu zebrano wszystkie informacje na temat dokumentacji, o której mowa w *Rozporządzeniu*, a także o przyjętych w .....
(nazwa placówki oświatowej)
zasadach i procedurach przetwarzania danych osobowych.

PRYWATNE PRZEDSZKOLE
PIOTRUSIA PANA
ul. Żabiniec 45, 31-215 Kraków
tel. 12 416-37-67

Jeśli w trakcie działania organizacji będą zachodziły zmiany w niniejszych regulacjach (zarówno w oparciu o przepisy prawa, jak również w związku ze zmianami i zapotrzebowaniem wynikającym z bieżącego funkcjonowania organizacji), będą one znajdowały odzwierciedlenie w niniejszej Polityce, w formie nowych załączników lub aktualizacji treści załączników uwzględnionych w niej obecnie.

Zakres przedmiotowy stosowania Polityki Ochrony Danych Osobowych obejmuje wszystkie czynności przetwarzania danych osobowych realizowane przez Administratora zarówno wewnątrz jak i na zewnątrz Organizacji, z wykorzystaniem danych zapisanych w formie elektronicznej jak i papierowej.

Zakres podmiotowy niniejszej dokumentacji obejmuje wszystkich pracowników i współpracowników Administratora, realizujące w jego imieniu i na jego rzecz czynności przetwarzania danych osobowych przez niego administrowanych.

Podstawa prawna

Zasady przetwarzania danych osobowych w szczególności regulują:

- *Rozporządzenie 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*
- *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz. U. z 2018 r. poz. 1000)
- *Ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679* (obecnie jeszcze w fazie projektu).

Polityka ochrony danych osobowych jest dokumentem poufnym i nie może być udostępniana podmiotom trzecim bez wcześniejszej zgody administratora.

Celem Polityki ochrony danych osobowych jest ustalenie zasad bezpieczeństwa przetwarzania danych osobowych, których przestrzeganie i realne stosowane przez wszystkich pracowników i współpracowników Organizacji. Ma to zapewnić bezpieczeństwo danych osobowych w niej przetwarzanych. Polityka określa zasady pracy z wykorzystaniem zbiorów danych osobowych przetwarzanych tradycyjnie w postaci papierowej, jak również w systemach informatycznych.

Zgodnie z wytycznymi wynikającymi z *Rozporządzenia*, administrator stosuje w procesie przetwarzania tzw. podejście oparte na ryzyku (*risk based approach*). Wiąże się to z dokonywaniem ciągłej oceny ryzyka i w sytuacjach, gdy ADO wprowadza zmiany do procesu przetwarzania danych lub wynikają one z zewnętrznych czynników, każdorazowo z przeprowadzeniem analizy ryzyka. Należy w niej uwzględnić ryzyko naruszenia praw i wolności osób, których dane administrator przetwarza, jak również ryzyko, jakie niesie to dla organizacji. W wyniku tej analizy administrator podejmie decyzje o rodzaju wdrażanych organizacyjnych i technicznych środków ochrony danych osobowych i konieczności przeprowadzenia pogłębionej analizy ryzyka tzw. oceny skutków dla ochrony danych osobowych.

Rodzaj wdrożonych zabezpieczeń poza zidentyfikowanym poziomem ryzyka uzależniony jest od dostępności najnowszych rozwiązań technologicznych i możliwości budżetowych ADO.

Szczegółowe wytyczne dotyczące stosowanych przez administratora zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych zawiera Załącznik: Instrukcja zarządzania systemem informatycznym.

II Definicje

Organizacja – podmiot wskazany na pierwszej tytułowej stronie Polityki, dla celów którego niniejsza Polityka zostaje opracowana i wdrożona.

Polityka – niniejszy dokument Polityki bezpieczeństwa danych osobowych.

ADO – administrator danych osobowych; osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i środki przetwarzania danych osobowych.

IOD – inspektor ochrony danych, wyznaczony spośród pracowników administratora lub współpracujący z administratorem na zasadach outsourcingu specjalista nadzorujący stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych dobranych stosownie do zagrożeń oraz kategorii danych objętych ochroną.

ASI – administrator systemu informatycznego, wyznaczony przez administratora danych osobowych specjalista odpowiedzialny za prawidłowe funkcjonowanie sprzętu, oprogramowania i ich konserwację, w zakresie wskazanym przez ADO. (RODO nie wskazuje na konieczność wyznaczenia ASI, w wielu organizacjach został on już powołany na bazie poprzedniej *Ustawy o ochronie danych osobowych*, warto więc to wykorzystać. Dobrze jest mieć w organizacji jedną osobę nadzorującą funkcjonowanie działu IT).

PUODO – Prezes Urzędu Ochrony Danych Osobowych, będący organem powołanym do spraw z zakresu ochrony danych osobowych.

UODO – organ nadzorczy – Urząd Ochrony Danych Osobowych.

Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m.in. o umowę powierzenia.

Strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe.

Podmiot przetwarzający (procesor) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Użytkownik – osoba korzystająca w procesie realizacji zadań z systemu informatycznego administratora, posiadająca indywidualny login i hasło do systemu, rozpoczynająca w nim pracę uwierzytelnieniem.

Ustawa – *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz.U. z 2018 r. poz. 1000).

RODO – *Rozporządzenie 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 /Dz. Urz. UE.L nr 119.*

Dane osobowe zwykłe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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.

Dane szczególnie chronione – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej oraz dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

Zbiór danych osobowych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Przetwarzane danych – operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie,

przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie itd.

OSOD – DPIA (*Data Protection Impact Assessment*) – ocena skutków dla ochrony danych. Proces pozwalający ocenić, czy przetwarzanie danych w ramach określonej czynności niesie za sobą wysokie ryzyko, czy wdrożone środki ochrony pozwolą je zniwelować.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

System tradycyjny – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze.

Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Identyfikator użytkownika (login) – identyfikujący użytkownika systemów informatycznych ciąg znaków literowych, cyfrowych lub innych.

Hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Usuwanie danych – zniszczenie danych osobowych lub ich modyfikacja, która uniemożliwia ustalenie tożsamości osoby, której dane dotyczą.

Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

III Dane osobowe

3.1. Zgodnie z definicją zapisaną w RODO dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, czyli 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.

Przy rozstrzyganiu, czy określona informacja lub informacje stanowią dane osobowe, administrator dokonuje zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby.

3.2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, np. przez odwołanie się do konkretnego numeru identyfikacyjnego lub specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne danej osoby. Danymi osobowymi będą zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań wystarczające do jej ustalenia.

3.3 Wyróżniamy dane osobowe zwykłe i dane osobowe wymagające szczególnej ochrony. Do tych zalicza się dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, czyli informacji o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej, dane dotyczące seksualności lub orientacji seksualnej osoby, do której należą.

Kraków 25 V 2018 r.

DYREKTOR
PRYWATNEGO PRZEDSZKOLA
PIOTRUSIA PANA
w KRAKOWIE
mgr Barbara Tarapacz