Żłobek Miejski w Koszalinie

**Polityka ochrony danych osobowych**

Zatwierdził:

…………………………………………

(data, podpis)

Niniejszy dokument jest Polityką Ochrony Danych Osobowych w rozumieniu RODO – Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 119, s.1).

Zawiera on:

1. opis zasad ochrony danych obowiązujących w Żłobku Miejskim w Koszalinie.
2. odwołania do procedur i instrukcji dotyczących poszczególnych obszarów ochrony danych osobowych.

Polityka Ochrony Danych Osobowych została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymaganiami RODO.

Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Dyrektor Żłobka. Za nadzór i monitorowanie przestrzegania Polityki odpowiada wydzielony pracownik pełniący rlę Inspektora Ochrony Danych. Do stosowania Polityki zobowiązani są wszyscy pracownicy przetwarzający dane osobowe.

**§ 1 Skróty i definicje**

Stosowane w niniejszym dokumencie skróty i definicje oznaczają:

1. Polityka oznacza niniejszą Politykę bezpieczeństwa, o ile co innego nie wynika wyraźnie z kontekstu,
2. RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1),
3. Dane osobowe oznaczają wszystkie informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych,
4. Dane wrażliwe oznaczają dane specjalne i dane karne,
5. Dane specjalne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej,
6. Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa,
7. Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu,
8. Podmiot przetwarzający oznacza organizację lub osobę, której Przedszkole powierzyło przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość),
9. Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się,
10. Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej,
11. IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych,
12. RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych,
13. Administrator Danych oznacza Żłobek Miejski w Koszalinie.

**§ 2 Inspektor Ochrony Danych**

1. Administrator Danych jest podmiotem publicznym, który na mocy art. 37 ust. 1 RODO ma obowiązek powołania Inspektora Ochrony Danych (IOD).
2. Osoba powołana na stanowisko IOD posiada:
   1. odpowiednią wiedzę fachową tj. gruntowną wiedzę na temat krajowego i europejskiego prawa oraz praktyk w dziedzinie ochrony danych osobowych,
   2. znajomość struktury administratora oraz wiedzę o dokonywanych czynnościach przetwarzania a także o systemach informatycznych oraz o potrzebach administratora w zakresie bezpieczeństwa i ochrony danych,
   3. znajomość przepisów administracyjnych oraz postępowania administracyjnego w jednostce organizacyjnej,

i odpowiednie cechy osobowe tj. uczciwość i wysoko rozwiniętą etykę zawodową.

1. IOD jest zatrudniony na podstawie umowy o pracę i został powołany dokumentem „Wyznaczenie Inspektora Ochrony Danych”.
2. IOD podlega bezpośrednio Dyrektorowi Żłobka.
3. Administrator danych zapewnia, że dodatkowe zadania i obowiązki, które realizuje IOD nie powodują konfliktu interesów.
4. Administrator Danych zapewnia niezbędne zasoby dla IOD przez co rozumie się między innymi:
   1. - zapewnienie wystarczającej ilości czasu,
   2. - szkolenia i inne formy doskonalenia zawodowego
5. IOD wykonuje obowiązki wskazane w art. 39 RODO.

**§ 3 Zasady ochrony przetwarzania danych osobowych**

Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:

1. w oparciu o podstawę prawną i zgodnie z prawem,
2. rzetelnie i uczciwie,
3. w sposób przejrzysty dla osoby, której dane dotyczą,
4. w konkretnych celach,
5. tylko niezbędne dane,
6. nie dłużej niż trzeba,
7. zapewniając odpowiednie bezpieczeństwo danych.

**§ 4 System ochrony danych**

Na system ochrony danych osobowych składają się następujące elementy:

1. zidentyfikowane zbiory danych osobowych oraz opis sposobów ich przetwarzania,
2. Rejestr Czynności Przetwarzania Danych Osobowych,
3. podstawy prawne przetwarzania danych osobowych,
4. zasady realizacji obowiązku informacyjnego,
5. procedury obsługi praw osób, których dane są przetwarzane,
6. metody zarządzania minimalizacją przetwarzanych danych,
7. procedury zapewniające odpowiedni poziom bezpieczeństwa danych,
8. zasady identyfikacji i obsługi incydentów,
9. procedura przywrócenia dostępności danych osobowych w razie wystąpienia incydentu,
10. zasady powierzania przetwarzania danych podmiotom zewnętrznym,
11. zasady uruchamiania nowych projektów, w ramach których będą przetwarzane dane osobowe.

4.1. Identyfikacja zbiorów danych osobowych

Administrator danych zidentyfikował procesy i zbiory, w których są przetwarzane dane osobowe. Dla każdego zbioru wskazano właściciela i zweryfikowano czy nie zachodzi przypadek współadministrowania. W ramach przeprowadzonej inwentaryzacji zostały wskazane grupy informacji przetwarzane w zbiorach. W ramach każdego zbioru dokonano analizy związanej z przetwarzaniem szczególnych kategorii danych osobowych oraz ewentualnym profilowaniem. W ramach inwentaryzacji wskazano również aplikacje, które służą do przetwarzania danych.

Zinwentaryzowane zbiory zostały opisane w „Wykazie zbiorów w których przetwarzane są dane osobowe”, który zawiera informacje wskazane w zał. nr 1 do niniejszej Polityki.

4.2. Rejestr Czynności Przetwarzania Danych Osobowych

Administrator danych prowadzi, zgodnie z wymaganiami art. 30 RODO, Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr stanowi formę dokumentowania czynności przetwarzania danych osobowych. Za prowadzenie Rejestru odpowiada IOD. Rejestr jest aktualizowany w przypadku podjęcia przez Administratora nowych czynności przetwarzania danych. Wzór Rejestru Czynności Przetwarzania Danych stanowi zał. nr 2 do Polityki.

Niektóre dane osobowe są przetwarzane w Żłobku Miejskim w Koszalinie na podstawie umowy powierzenia przetwarzania. Rejestr dla tych danych prowadzony jest zgodnie z wzorem stanowiącym zał. nr 3 do Polityki.

4.3. Podstawy prawne przetwarzania danych osobowych

Administrator dokumentuje w Wykazie zbiorów, o którym mowa w pkt. 4.1. podstawy prawne przetwarzania danych osobowych dla poszczególnych zbiorów. W przypadku każdego zbioru wskazuje podstawę prawną przetwarzania danych zwykłych i szczególnych kategorii danych osobowych, które wynikają z RODO (np. zgoda, umowa czy obowiązek prawny) i dookreśla je dodatkowymi informacjami np. dla zgody wskazując na jej zakres a w przypadku podstawy prawnej konkretny przepis ustawy branżowej. Podstawy prawne są okresowo weryfikowane.

4.4. Zasady realizacji obowiązku informacyjnego

Przy pozyskiwaniu danych osobowych od osoby, której dane dotyczą Administrator spełnia obowiązek informacyjny opisany w art. 13 RODO.

W przypadku pozyskiwania danych od potencjalnych pracowników, Administrator przekazuje podstawowe informacje dotyczące przetwarzania danych w ogłoszeniu o rozpoczęciu rekrutacji i przy przyjmowaniu CV.

Przy zbieraniu danych od pracowników obowiązek informacyjny realizowany jest przez udostępnienie informacji o przetwarzaniu danych pracownika w formie dokumentu i potwierdzenie jej odebrania przez złożenie podpisu pod stosownym oświadczeniem. W stosunku do osób zatrudnionych u Administratora w dniu wejścia w życie niniejszej Polityki obowiązek informacyjny został zrealizowany przez udostępnienie klauzuli każdemu pracownikowi i potwierdzenie podpisem możliwości zapoznania się.

W przypadku pozyskiwania danych osobowych od rodziców (dane osobowe rodziców i dzieci), każdy z nich ma możliwość zapoznania się z odpowiednią klauzulą informacyjną wywieszoną na tablicy ogłoszeń w siedzibie administratora, u Dyrektora i jego Zastępców oraz opublikowaną w BIP-ie zakładu.

Pozostałe klauzule informacyjne dotyczące funkcjonowania żłobka znajdują się u Dyrektora, jego Zastępców oraz są publikowane w BIP-ie.

Administrator nie pozyskuje danych osobowych w inny sposób, niż od osoby, której one dotyczą.

4.5. Procedury obsługi praw osób, których dane są przetwarzane

W celu właściwej obsługi praw osób, których dane są przetwarzane przez Administratora, została opracowana Procedura obsługi żądań podmiotu danych, która stanowi załącznik nr 3 do niniejszego dokumentu.

4.6. Metody zarządzania minimalizacją przetwarzanych danych

Na minimalizację przetwarzania danych mają wpływ następujące czynniki:

- adekwatność danych w stosunku do celu przetwarzania,

- dostęp do danych tylko dla tych osób i w takim zakresie jak jest to niezbędne,

- przechowywanie danych nie dłużej niż jest to niezbędne.

W ramach wdrażania RODO Administrator zweryfikował zakres pozyskiwanych informacji oraz zakres ich przetwarzania pod kątem adekwatności w stosunku do celu. Administrator zobowiązał właścicieli danych osobowych do okresowego przeglądu pozyskiwanych i przetwarzanych danych osobowych, by zapewnić, że ich zakres nie wykracza ponad niezbędne minimum. W celu wywiązania się z tego zadania, właściciel danych powinien między innymi zweryfikować, czy nie nastąpiły zmiany w przepisach prawa.

W celu minimalizacji dostępu do danych osobowych Administrator stosuje ograniczenia organizacyjne, fizyczne i logiczne. Ograniczenia organizacyjne realizowane są poprzez odbieranie od pracowników zobowiązań o zachowaniu poufności i określanie zakresu upoważnień do przetwarzania danych. Ograniczenia fizyczne wynikają z reglamentacji dostępu do pomieszczeń i dokumentów. Ograniczenia logiczne realizowane są przez nadawanie odpowiednich uprawnień dostępowych do zasobów sieciowych i systemów, w których są przetwarzane dane osobowe. Uprawnienia dostępowe są aktualizowane przy zmianie stanowiska lub roli pracownika w procesie przetwarzania danych. Administrator zapewnia, że przynajmniej raz do roku dokonuje przeglądu użytkowników systemów i nadanych im uprawnień. Szczegółowe zasady zarządzania uprawnieniami zostały opisane w Procedurze nadawania i zmiany uprawnień.

Administrator zarządza cyklem życia dokumentów. Instrukcja kancelaryjna określa zarówno okres przechowywania dokumentów na stanowisku pracy jak i okres ich archiwizacji. Administrator zapewnia, że dokumenty przechowywane w archiwum są poddawane okresowym przeglądom i że są niszczone w bezpieczny sposób po upływie okresu ich przechowywania.

4.7. Procedury zapewniające odpowiedni poziom bezpieczeństwa

Administrator zapewnia odpowiedni poziom bezpieczeństwa danych osobowych przez:

- zapewnienie odpowiedniego stanu wiedzy o bezpieczeństwie i zagrożeniach wynikających z przetwarzania danych osobowych (szkolenia pracowników),

- okresowe przeprowadzanie analizy ryzyka i dobór możliwych do zastosowania zabezpieczeń technicznych i organizacyjnych zgodnie z Procedurą analizy ryzyka (zał. nr 4),

- weryfikację skuteczności wdrożonych zabezpieczeń.

Administrator jest zwolniony z przeprowadzania oceny skutków dla ochrony danych dla tych operacji przetwarzania, które mają podstawę prawną w prawie polskim lub prawie UE.

Administrator dokonuje oceny skutków dla ochrony danych w tych operacjach, które wskazuje organ nadzorczy.

Po wdrożeniu nowych zabezpieczeń, ustanowionych w wyniku przeprowadzonej analizy ryzyka i ewentualnie oceny skutków dla ochrony danych osobowych administrator aktualizuje dokument Wykaz stosowanych zabezpieczeń.

4.8. Zasady identyfikacji i obsługi incydentów

Administrator przyjął zasady zobowiązujące wszystkich pracowników do powiadamiania o stwierdzeniu podatności systemu ochrony danych lub wystąpieniu incydentu bezpieczeństwa. Zasady te zostały opisane w Regulaminie ochrony danych osobowych.

Procedura obsługi naruszeń ochrony danych stanowi zał. nr 5 do Polityki.

4.9. Zasady powierzania przetwarzania danych podmiotom zewnętrznym

Administrator opracował ankietę, na podstawie której weryfikuje nowe firmy, z którymi zamierza podpisać umowy powierzenia przetwarzania danych osobowych (zał. nr 6 do Polityki). Weryfikacja firm ma zapewnić, że podmioty przetwarzające dają wystarczające gwarancje bezpiecznego przetwarzania danych osobowych.

Administrator opracował wzór umowy powierzenia przetwarzania danych osobowych, która stanowi załącznik nr 7 do Polityki.

Administrator prowadzi rejestr umów, na podstawie których powierzył przetwarzanie danych podmiotom zewnętrznym.

4.11. Zasady uruchamiania nowych projektów, w ramach których będą przetwarzane dane osobowe

W przypadku uruchamiania nowych projektów związanych z przetwarzaniem danych osobowych administrator zapewnia, że uwzględnia w nich zagadnienia związane z bezpieczeństwem i minimalizacją przetwarzanych danych.

**§ 5 Postanowienia końcowe**

1. Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych jest przeszkolony w zakresie RODO i wewnętrznych regulacji dotyczących ochrony danych osobowych.
2. Zbiór podstawowych zasad bezpiecznego przetwarzania danych osobowych został zapisany w Regulaminie ochrony danych osobowych (Zał. nr 8 do Polityki).
3. Po zapoznaniu się z zasadami ochrony danych osobowych, pracownik potwierdza znajomość tych zasad i deklaruje ich stosowanie.