POLITYKA OCHRONY DANYCH DLA

PRZEDSZKOLA NR 148

WROCŁAW 2025

Spis treści

ROZDZIAŁ I: WPROWADZENIE 2
ROZDZIAŁ II: OGÓLNA CHARAKTERYSTYKA DZIAŁALNOŚCI 2
ROZDZIAŁ III: ZASADY PRZETWARZANIA DANYCH OSOBOWYCH 7
ROZDZIAŁ IV: BEZPIECZEŃSTWO DANYCH 11

ROZDZIAŁ I: WPROWADZENIE

I. Niniejszym w Przedszkolu nr 148 we Wrocławiu, ul. Szkocka 64B, 54-402 Wrocław (dalej: **Placówka**) tworzy się spójny system zarządzania bezpieczeństwem informacji (dalej: **SZBI**), którego celem jest zapewnienie bezpieczeństwa informacji oraz ich wykorzystywanie zgodnie z obowiązującym prawem. Na SZBI w Placówce składa się niniejsza Polityka Ochrony Danych oraz powiązane z nią wewnętrzne procedury i instrukcje.

II. Polityka Ochrony Danych uwzględnia wymogi wynikające z przepisów 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 (dalej: **RODO**), ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (dalej: **Ustawa**) oraz przepisów szczególnych. Polityka powinna podlegać okresowym aktualizacjom w miarę rozwoju prawa ochrony danych osobowych i praktyki jego stosowania w Polsce oraz w Unii Europejskiej.

III. Na Politykę Ochrony Danych składa się niniejszy dokument oraz załączniki:
1. Wzór rejestru czynności przetwarzania danych i wszystkich kategorii czynności przetwarzania
2. Wzór formularza testu interesu publicznego

IV. System zarządzania bezpieczeństwem informacji, w szczególności od strony dokumentów regulujących zasady postępowania, mające na celu zapewnienie bezpieczeństwa informacji zgromadzonych w Placówce, powinien podlegać regularnym przeglądom. Polityka Ochrony Danych, oraz powiązane z nią procedury i instrukcje, powinna być poddawana okresowym weryfikacjom pod kątem aktualności oraz kompletności, mając na względzie zmiany zachodzące w Placówce, obowiązujących ją przepisach prawa oraz dostosowanie wewnętrznych regulacji do wytycznych organów i najlepszych praktyk rynkowych w sektorze publicznym.

ROZDZIAŁ II: OGÓLNA CHARAKTERYSTYKA DZIAŁALNOŚCI

A. Podstawy prawne działalności Placówki

Placówka jest publiczną jednostką oświatową Gminy Wrocław. Placówkę tworzy:

a) Przedszkole

Działa na podstawie obowiązujących przepisów prawa, w tym w szczególności na podstawie:

1. ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe;
2. ustawy z dnia 7 września 1991 r, o systemie oświaty;

3. rozporządzenia Ministra Edukacji Narodowej z 17 marca 2017 r. w sprawie szczegółowej organizacji publicznych szkół i publicznych przedszkoli;
4. rozporządzenia Ministra Edukacji Narodowej z 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły policealnej;
5. rozporządzenia Ministra Edukacji Narodowej z 7 czerwca 2017 r. zmieniające rozporządzenie w sprawie warunków i sposobu organizowania religii w publicznych przedszkolach i szkołach;
6. rozporządzenia Ministra Edukacji Narodowej z 25 sierpnia 2017 r. w sprawie zasad organizacji i udzielania pomocy psychologiczno-pedagogicznej w publicznych przedszkolach i szkołach;
7. rozporządzenia Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji;
8. swojego aktu założycielskiego oraz swojego statutu.

B. Cele działalności

Cele Placówki są wypadkową realizowanej przez nią szeroko pojętej działalności edukacyjnej. Do podstawowych zadań należy zapewnienie warunków wszechstronnego rozwoju uczniów, osiąganego poprzez realizację zadań w zakresie nauczania, kształcenia umiejętności oraz wychowania, z uwzględnieniem zasad bezpieczeństwa, a także zasad promocji i ochrony zdrowia.
Placówka przetwarza dane osobowe w celach:

1. realizacji zadań dydaktycznych, wychowawczych i opiekuńczych,
2. prowadzenia dokumentacji,
3. zapewnienia bezpieczeństwa uczniów i pracowników,
4. realizacji innych obowiązków prawnych i sprawozdawczych.

Cele te Placówka osiąga m.in. poprzez
- w obszarze działalności Przedszkola:

1. Wspomaganie dzieci w rozwijaniu uzdolnień oraz kształtowanie czynności intelektualnych potrzebnych im w codziennych sytuacjach i w dalszej edukacji.
2. Budowanie systemu wartości, w tym wychowanie dzieci tak, żeby lepiej orientowały się w tym, co jest dobre, a co złe.
3. Kształtowanie u dzieci odporności emocjonalnej koniecznej do racjonalnego radzenia sobie w nowych i trudnych sytuacjach, w tym także do łagodnego znoszenia stresów i porażek.
4. Rozwijanie umiejętności społecznych dzieci, które są niezbędne w poprawnych relacjach z dziećmi i dorosłymi.
5. Stwarzanie warunków sprzyjających wspólnej i zgodnej zabawie oraz nauce dzieci o zróżnicowanych możliwościach fizycznych i intelektualnych.
6. Troska o zdrowie dzieci i ich sprawność fizyczną; zachęcanie do uczestnictwa w zabawach i grach sportowych.
7. Budowanie dziecięcej wiedzy o świecie społecznym, przyrodniczym i technicznym oraz rozwijanie umiejętności prezentowania swoich przemyśleń w sposób zrozumiały dla innych.
8. Wprowadzenie dzieci w świat wartości estetycznych i rozwijanie umiejętności wypowiadania się poprzez muzykę, małe formy teatralne oraz sztuki plastyczne.

9. Kształtowanie u dzieci poczucia przynależności społecznej (do rodziny, grupy rówieśniczej i wspólnoty narodowej) oraz postawy patriotycznej.
10. Zapewnienie dzieciom lepszych szans edukacyjnych poprzez wspieranie ich ciekawości, aktywności i samodzielności, a także kształtowanie tych wiadomości i umiejętności, które są ważne w edukacji szkolnej.

C. Odpowiedzialność

1. **Dyrektor Placówki odpowiada za:**
   - wydawanie zarządzeń regulujących obowiązki związane z działalnością SZBI, w tym dotyczące kwestii proceduralnych i porządkowych;
   - wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymywanie i ciągłe doskonalenie SZBI;
   - wspieranie procesowego podejścia do zarządzania ochroną danych oraz angażuje się w działania promujące SZBI;
   - podejmuje kluczowe decyzje dotyczące funkcjonowania POD;
   - wyznacza Inspektora Ochrony Danych;
   - nadzoruje pracę Inspektora Ochrony Danych;
   - zatwierdza wyniki oceny ryzyka oraz plan postępowania z ryzykiem;
   - uczestniczy w przeglądzie zarządzania i zatwierdza raport z przeglądu zarządzania dla Placówki.

2. **Inspektor Ochrony Danych odpowiada za:**
   - informowanie Dyrektora Placówki oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   - monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk i instrukcji Placówki w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   - udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania (stosownie do przepisów art. 35 RODO);
   - współpracę z organami nadzorczymi w obszarze ochrony danych osobowych, ze szczególnym uwzględnieniem Prezesa Urzędu Ochrony Danych Osobowych;
   - pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Inspektor Ochrony Danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Inspektor Ochrony Danych podlega bezpośrednio najwyższemu kierownictwu administratora, tj. dyrekcji, dlatego też został umiejscowiony w strukturze organizacyjnej Placówki. Jego dane, obejmujące imię, nazwisko oraz adres poczty elektronicznej oraz dane jego zastępcy, dostępne są na stronie www Placówki https://przedszkole148.edu.wroclaw.pl/ w zakładce Kontakt.

3. **Wszyscy pracownicy Placówki:**
   - odpowiadają za bezpieczeństwo informacji, które zostały im udostępnione;

- powinni przetwarzać wyłącznie te informacje, które są niezbędne dla realizacji ich obowiązków służbowych;
- są zobowiązani do stosowania się do zasad bezpieczeństwa informacji i ochrony danych osobowych obowiązujących w Placówce;
- biorą udział w regularnych szkoleniach z zakresu bezpieczeństwa informacji zapewnianych przez Placówkę.

D. Kategorie osób, których dane są przetwarzane przez Placówkę

W obszarze przetwarzania danych osobowych działalność Placówki skupia się na przetwarzaniu danych osobowych:

1. dzieci i uczniów aplikujących do uczęszczania do Placówki oraz ich rodziców lub opiekunów prawnych;
2. dzieci i uczniów uczęszczających do Placówki oraz ich rodziców lub opiekunów prawnych;
3. dzieci i uczniów biorących udział w konkursach i olimpiadach organizowanych przez Placówkę;
4. absolwentów Placówki oraz ich rodziców lub opiekunów prawnych;
5. kadry pedagogicznej odpowiedzialnej za edukację dzieci uczęszczających do Placówki;
6. kadry administracyjnej odpowiedzialnej za bieżące funkcjonowanie Placówki;
7. innych osób z najbliższego otoczenia Placówki – najemców pomieszczeń, dostawców, wykonawców, kandydatów do pracy.

E. Placówka jako administrator czy jako procesor

Z uwagi na fakt, że Placówka świadczy usługi edukacyjne w wykonaniu postanowień aktu założycielskiego, statutu oraz powszechnie obowiązujących przepisów prawa, które nakładają na nią określone obowiązki, należy uznać, że w świetle art. 4 pkt 7 RODO to Placówka odpowiada za cele i sposoby przetwarzania danych osobowych. Tym samym generalnie w procesach przetwarzania danych realizowanych w swojej działalności Placówka będzie uznawana za administratora.

Na zasadzie wyjątku Placówka może występować jako podmiot przetwarzający – tzw. procesor (czyli podmiot, który przetwarza dane osobowe w imieniu i na zlecenie administratora). Zasady postępowania, w przypadku, gdy Placówka staje się podmiotem przetwarzającym zostały określone w Procedurze – placówka oświatowa jako podmiot przetwarzający. Procesy, przy realizacji których, dochodzi do przetwarzania danych osobowych, zostały zidentyfikowane i zebrane w ramach Rejestru Czynności Przetwarzania Danych (gdzie Placówka występuje jako administrator) oraz Rejestru Wszystkich Kategorii Czynności Przetwarzania (Placówka w roli procesora), prowadzonymi stosownie do art. 30 ust. 1 oraz art. 30 ust. 2 RODO. Nadzór na Rejestrami sprawuje Inspektor Ochrony Danych.

F. Status Rady Rodziców

Placówka uznaje, że Rada Rodziców w obszarze swojej podstawowej działalności co do zasady nie spełnia kryteriów do uznania za odrębnego od Placówki administratora danych (kryterium samodzielnego decydowania o celach i środkach przetwarzania danych osobowych co do zasady nie zostaje spełnione). Z tej perspektywy członkowie Rady Rodziców otrzymują upoważnienia do przetwarzania danych osobowych.

Jednocześnie należy wskazać, że Placówka w określonych przypadkach będzie uznawać Radę Rodziców (jej członków działających w otoczeniu Placówki) za odrębnego administratora danych, który jest obowiązany do samodzielnego zadbania o prawidłowość przetwarzania danych osobowych. Dotyczyć to będzie w szczególności:

1. przypadków, gdy sposób funkcjonowania Rady Rodziców w sposób istotny oddzieli się od Placówki – w szczególności prace Rady Rodziców będą odbywały się poza Placówką, poza Placówką będzie przechowywana dokumentacja zawierająca dane osobowe, Rada Rodziców będzie odmawiać prawa do nadzoru Rady ze strony Inspektora Ochrony Danych lub będzie odmawiać zastosowania się do jego wskazań;
2. dla procesów przetwarzania, w których Rada Rodziców będzie działała całkowicie z własnej inicjatywy poza auspicjami Placówki – np. prowadzenie samodzielnego profilu w mediach społecznościowych (np. fanpage Rady Rodziców na Facebooku) lub inne przypadki samodzielnego publikowania danych osobowych (uczniów, nauczycieli).

G. Powierzanie danych osobowych podwykonawcom

Zgodnie z artykułem 28 RODO, jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą. Przetwarzanie danych osobowych przez podmiot przetwarzający może odbywać się wyłącznie na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora.

RODO w art. 28 ust. 3 określa szczegółowe wymagania jakie powinna określać odpowiednio sformułowana umowa przetwarzania danych osobowych. Co istotne RODO w swojej treści nie posługuje się pojęciem „Umowy powierzenia", znanym z art. 31 ustawy o ochronie danych osobowych z 1997 roku, jednocześnie nazewnictwo takie zostało przyjęte przez Placówkę w związku z obowiązującą na rynku utrwaloną praktyką w tym obszarze.

Zidentyfikowano obszary, w których Placówka trwale lub często powierza przetwarzanie danych osobowych. W ramach wspomnianych obszarów można przykładowo wskazać współpracę z podmiotami zapewniającymi

1. obsługę IT
2. obsługę prawną
3. utylizację dokumentów
4. obsługę strony www
5. oprogramowanie bazodanowe
6. usługi fotografa
7. dziennik elektroniczny
8. legitymacje dla uczniów i nauczycieli.

Dla powyższych przypadków Placówka posiada ogólny wzór umowy powierzenia przetwarzania danych osobowych, który każdorazowo jest dostosowywany do danej współpracy, a dla wybranych z nich został wypracowany gotowy wzór przy wsparciu IOD. Dodatkowo Placówka prowadzi wykaz podmiotów przetwarzających, w ramach którego ewidencjonuje zawierane umowy, kontrolując proces powierzenia.

Mając na uwadze, że Placówka jest wrocławską placówką oświatową istotna bieżąca współpraca w obszarze powierzania danych może być realizowana z Centrum Usług Informatycznych (CUI), ul. Namysłowska 8, 50-304 Wrocław. Taka współpraca odbywa się zawsze z uwzględnieniem warunków określonych w art. 28 RODO.

Ponadto w ramach organizowanych konkursów mogą zdarzać się przypadki powierzenia danych uczestników innym placówkom oświatowym, które zgłaszają uczestnictwo w konkursie. Obowiązek przedstawienia formularza rodzicom/przedstawicielom ustawowym, oraz zapewnienie jego podpisania ciąży zazwyczaj na placówce – uczestniku, która następnie ma obowiązek przekazać odpowiednio wypełniony formularz Placówki – organizatorowi. Taka praktyka w świetle art. 28 RODO oznacza, że placówka – uczestnik w zakresie w jakim zapewnia wypełnienie formularza zgody na udział ucznia w zewnętrznym etapie Konkursu działa jako podmiot przetwarzający dane osobowe na rzecz Placówki – organizatora. W świetle art. 28 ust. 3 RODO taka sytuacja oznacza, że Placówka – organizator powinna zapewnić podpisanie umowy powierzenia przetwarzania danych osobowych ze wszystkimi placówkami – uczestnikami, albo powinna w tym zakresie wykorzystać tzw. „inny instrument prawny".

H. Udostępnianie danych przez Placówkę innym podmiotom

Działalność Placówki nie wiąże się z koniecznością przetwarzania danych osobowych na masową skalę. Placówka nie udostępnia danych osobowych innym podmiotom w celach komercyjnych. Pozostaje jednak jednostką oświatową Gminy Wrocław, która jest zobowiązana do przekazywania określonych raportów oraz informacji do poszczególnych Wydziałów Urzędu Miejskiego Wrocławia, zgodnie z powszechnie obowiązującymi przepisami prawa oraz regulacjami prawa miejscowego.

Ponadto udostępnianie danych osobowych ma również miejsce w przypadku podejmowania przez Placówkę współpracy z ośrodkami medycznymi, które angażują się w określone badania zdrowotne uczniów (np. badania skóry, badania słuchu, wzroku, uzębienie). W tych przypadkach administratorem danych osobowych jest podmiot przeprowadzający dane badanie, działający za zgodą Placówki oraz rodziców lub przedstawicieli prawnych uczniów.

Placówka może również przekazywać dane osobowe w związku z koniecznością dopełnienia obowiązków prawnych właściwym instytucjom publicznym (np. Zakładowi Ubezpieczeń Społecznych, urzędom skarbowym, sądom, Policji, Prokuraturze itp.).

ROZDZIAŁ III: ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Placówka przy przetwarzaniu danych osobowych stosuje się do następujących zasad:

- Zasady legalności i rzetelności – Placówka przetwarza dane osobowe zgodnie z obowiązującym prawem, w tym zgodnie z całokształtem przepisów RODO i podchodzi do tego w sposób rzetelny.
- Zasady transparentności (przejrzystości) – Placówka spełnia obowiązek informacyjny wobec osób, których dane przetwarza.
- Zasady ograniczenia celu oraz minimalizacji danych osobowych – Placówka przetwarza dane osobowe zawsze w konkretnych, wyraźnych i prawnie uzasadnionych celach.
- Zasady prawidłowości – Placówka dba o to, aby dane osobowe, które przetwarza, były aktualne i zgodne z prawdą. Dlatego niezwłocznie reaguje na każdy wniosek o ich sprostowanie czy

aktualizację, a także na wiarygodny sygnał, że przetwarzane przez Placówkę dane osobowe mogą być nieprawidłowe.

- Zasady ograniczenia przechowywania danych osobowych – Placówka przechowuje dane osobowe tak długo, jak to jest niezbędne do celów, w których dane osobowe te są przetwarzane. Placówka ustala konkretny okres przechowywania danych osobowych, a po jego upływie dane osobowe trwale usuwa, niszczy lub anonimizuje.
- Zasady rozliczalności – Placówka przetwarza dane osobowe tak, aby być w stanie wykazać, że odbywa się to zgodnie z obowiązującymi przepisami prawa oraz zasadami opisanymi w niniejszej Polityce Ochrony Danych. Placówka dokumentuje to, w jaki sposób przetwarza dane osobowe.

Szczegółowe informacje o realizowaniu przez Placówkę powyższych zasad zostały ujęte w kolejnych punktach.

A. Przetwarzanie przez Placówkę danych wrażliwych

Przetwarzane przez Placówkę dane osobowe generalnie nie mają charakteru wrażliwego. Dane wrażliwe pojawiają się jednak w przypadku, gdy wychowankowie lub uczniowie mają jakieś schorzenia lub przewlekłe choroby, w przypadkach, gdy rodzice deklarują chęć uczestnictwa dziecka w zajęciach religii, w obszarze przetwarzania danych osobowych pracowników w zakresie ich zdrowotnych zdolności do pracy – w zakresie wymaganym przez przepisy polskiego prawa. Elementy danych wrażliwych pojawiają się również w tym przypadkach, gdzie Placówka aktywnie działa w zakresie wsparcia psychologiczno-pedagogicznego i w tym zakresie pozyskuje dodatkowe dane o uczniu i/lub jego sytuacji rodzinnej. W przypadkach uczeń kierowany jest jednak do odrębnej placówki – Poradni Psychologiczno – Pedagogicznej funkcjonującej na terenie Wrocławia.

B. Przetwarzanie danych osobowych dotyczących wyroków skazujących i czynów zabronionych

Wymaga wskazania, że w przypadku zatrudniania osób na stanowiska nauczycieli, zgodnie z art. 10 ust. 5 ustawy – Karta nauczyciela, zbierane są od przyszłych pracowników zaświadczenia o niekaralności wydawane przez Krajowy Rejestr Karny.

Dodatkowo na podstawie art. 21 ust. 1 ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich *przed nawiązaniem z osobą stosunku pracy lub przed dopuszczeniem osoby do innej działalności związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi na pracodawcy lub innym organizatorze w zakresie takiej działalności oraz na osobie, z którą ma być nawiązany stosunek pracy lub która ma być dopuszczona do takiej działalności, ciążą obowiązki określone w ust. 2-8.*

Pracodawca lub inny organizator są obowiązani do uzyskania informacji, czy dane takiej osoby są zamieszczone w Rejestrze z dostępem ograniczonym lub w Rejestrze osób, stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 wydała postanowienie o wpisie w Rejestrze. Dlatego też, Dyrektor Placówki przed zatrudnieniem nowych pracowników, zasięga informacji, czy dane tych osób są zgromadzone w Rejestrze Sprawców Przestępstw na Tle Seksualnym.

Dodatkowo Placówka otrzymuje od osoby, z która ma być nawiązany stosunek pracy lub która ma być dopuszczona do ww. opisanej działalności, informację z Krajowego Rejestru Karnego w zakresie przestępstw określonych w rozdziale XIX i XXV Kodeksu karnego, w art. 189a i art. 207 Kodeksu karnego oraz w ustawie z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii, lub za odpowiadające tym przestępstwom czyny zabronione określone w przepisach prawa obcego. Tym samym Placówka zbiera w swoich systemach dane dotyczące wyroków skazujących i czynów zabronionych (art. 10 RODO).

Nadto w świetle art. 10 ust. 8b Karty Nauczyciela, Dyrektor Placówki, przed nawiązaniem stosunku pracy z nauczycielem, jest obowiązany zasięgnąć informacji z Centralnego Rejestru Orzeczeń Dyscyplinarnych, prowadzonego przez Ministra Edukacji Narodowej, czy nauczyciel nie był karany karą administracyjną, o której mowa w art. 10 ust. 5 pkt 4a Karty Nauczyciela. Dane o karze administracyjnej są zatem zbierane z powołaniem na art. 6 ust. 1 lit. c RODO.

C. Spełnianie obowiązku informacyjnego przez Placówkę

Zgodnie z art. 13 i 14 RODO Placówka ma obowiązek informować osoby, których dane dotyczą, o celach i sposobach przetwarzania ich danych osobowych. Określony powyżej obowiązek informacyjny jest jednym z najważniejszych obowiązków nakładanych przez RODO, które kładzie istotny nacisk na **transparentność** w procesach przetwarzania danych osobowych.

Placówka w przypadku pozyskiwania danych osobowych, przedstawia co najmniej za pomocą pierwszej warstwy informacyjnej najważniejsze informacje związane z przetwarzaniem danych osobowych, tj. podaje swoją tożsamość i dane kontaktowe, cele przetwarzania, prawa przysługujące w związku z przetwarzaniem danych osobowych, jak również informację o tym, gdzie (w jaki sposób) można uzyskać wszelkie informacje o przetwarzaniu danych osobowych, o których mowa w art. 13 (lub odpowiednio 14 RODO).

W celu stosowania transparentnej komunikacji w praktyce, Placówka przyjęła Instrukcję spełniania obowiązku informacyjnego.

D. Podstawy prawne przetwarzania danych osobowych przez Placówkę

Artykuł 6 RODO przewiduje sześć różnych podstaw prawnych przetwarzania danych osobowych. Placówka jako jednostka publiczna, co do zasady, nie może korzystać z podstawy prawnej przetwarzania jaką jest prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f ROD).

Placówka na co dzień przetwarza dane osobowe z powołaniem na następujące podstawy przetwarzania:

1. Wykonanie umowy (art. 6 ust. 1 lit. b RODO)
2. Wykonanie obowiązku wynikającego z przepisu prawa (art. 6 ust. 1 lit. c RODO) – Placówka w tym przypadku określa dokładny obowiązek wynikający z przepisów obowiązującego prawa krajowego, unijnego lub międzynarodowego.
3. Działanie w wykonaniu władzy publicznej lub w interesie publicznym (art. 6 ust. 1 lit e RODO) – Placówka w przypadku powołania się na klauzulę interesu publicznego lub władzy publicznej dokonuje najpierw rzetelnej analizy zwanej testem klauzuli interesu publicznego (załącznikiem do niniejszej Polityki jest wzór testu równoważenia) i określa ocenę zasadności procesu. Testy równoważenia dla procesów zdefiniowanych w Rejestrze Czynności Przetwarzania są przechowywane dla potrzeb rozliczalności wraz z dokumentacją dot. ochrony danych osobowych.

Działania z powołaniem na zgodę osoby, której dane dotyczą lub z powołaniem na ochronę żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, będą miały charakter wyjątkowy.

Działania z powołaniem na ochronę żywotnych interesów mają charakter wyjątkowy z tej przyczyny, że ta podstawa prawna dotyczy wpadkowych sytuacji, niecierpiących zwłoki, w których interesy jednostki przeważają w danej chwili nad ochroną jej prywatności. Jednocześnie administrator powinien w pierwszej możliwej chwili, kiedy tylko oddalone zostanie ryzyko dla interesów jednostki, znaleźć inną podstawę prawną przetwarzania.

Zgoda jako podstawa prawna przetwarzania ma dla działalności Placówki charakter wyjątkowy. Placówka będąc podmiotem publicznym działa generalnie z powołaniem na przepisy prawa, w tym w interesie publicznym.

Wychowankowie i uczniowie Placówki mogą brać udział w wielu konkursach w trakcie roku szkolnego. Część konkursów ma charakter wewnętrzny (tylko dla uczniów Placówki), a część konkursów ma charakter międzyprzedszkolny i międzyszkolny (regionalny, ponadregionalny, ogólnopolski).

Dla przypadków konkursów wewnętrznych Placówka nie musi realizować żadnych dodatkowych czynności w obszarze przetwarzania danych osobowych. W tym zakresie, zgodnie z przeprowadzonym testem klauzuli interesu publicznego Placówka działa w granicach swojej misji edukacyjnej, a podejmowane czynności przetwarzania danych osobowych nie wykraczają poza bieżące funkcjonowanie Placówki.

W przypadku pozostałych konkursów sytuacja przedstawia się już nieco inaczej. Tam, gdzie Placówka jako organizator konkursu zbiera dane osobowe uczniów innych placówek w celu realizacji konkursu, powinna uzyskać odrębną zgodę rodziców/przedstawicieli ustawowych uczniów na ich udział w konkursie. Taka zgoda w świetle art. 6 ust.1 lit. a RODO będzie oznaczała również zgodę na przetwarzanie danych osobowych tych uczniów w celu realizacji konkursu. Przy okazji zbierania takiej zgody Placówka zobowiązana jest wypełnić obowiązek informacyjny w rozumieniu art. 13 RODO. Jeżeli dodatkowo Placówka planuje publikować zdjęcia z przebiegu konkursu w Internecie, w mediach społecznościowych, zobowiązana jest uzyskać na to odrębną zgodę.

Jednocześnie zdiagnozowano przypadki działania w granicach interesu publicznego (funkcja wychowawcza Placówki, kształtowanie społeczności lokalnej, wykonywanie funkcji informacyjnej), które jednak mogą istotnie wpływać na prawa i interesy osób, których dane dotyczą.

Chodzi tutaj o przypadki publikowania wizerunków dzieci, uczniów i rodziców w sieci Internet. Działania takie, chociaż uzasadnione klauzulą interesu publicznego, wiążą się z upublicznieniem danych osobowych w taki sposób, że osoby których dane dotyczą mogą utracić kontrolę nad ich rozprzestrzenianiem się. Z tych przyczyn Placówka zdecydowała się dla tych przypadków przetwarzania danych uzyskiwać odrębną zgodę od osób, których dane dotyczą.

Zupełnie odrębnym przypadkiem, jest standardowo występująca w polskich przedszkolach i szkołach zgoda rodziców na udział ich dziecka w zajęciach religii. Oświadczenie takie ma charakter zgody, jednak jest to zgoda dotycząca udziału w zajęciach religii, a nie zgoda na przetwarzanie danych osobowych, w związku z udziałem w takich zajęciach. W analizowanym przypadku podstawą prawną przetwarzania danych osobowych dzieci są przepisy Rozporządzenia Ministra Edukacji Narodowej z dnia 14 kwietnia 1992 r. w sprawie warunków i sposobu organizowania nauki religii w publicznych przedszkolach i szkołach. Jeżeli rodzic, w trybie przewidzianym przez przepisy ww. Rozporządzenia wyrazi wolę udziału swojego

dziecka w zajęciach religii, to Placówka co do zasady jest zobowiązana zapewnić udział dziecka w zajęciach religii. Podstawą prawną przetwarzania danych osobowych dziecka w tym zakresie będzie art. 9 ust. 2 lit. g) RODO, zgodnie z którym przetwarzanie danych osobowych wrażliwych jest uprawnione w przypadku, gdy:

- *przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą*.

ROZDZIAŁ IV: BEZPIECZEŃSTWO DANYCH

A. Proces analizy ryzyka i postępowania z ryzykiem w Placówce

Regularnie i cyklicznie powinna być przeprowadzana w Placówce analiza ryzyka związanego z bezpieczeństwem przetwarzania danych. Celem tej analizy jest zapewnienie poufności, integralności, dostępności oraz autentyczności danych, jakie są przetwarzane przez Placówkę.

Placówka wypracowała reguły i metodę przeprowadzania analizy ryzyka, dokumentując jej rezultaty w formie pisemnej. Udokumentowane wyniki poszczególnych analiz są przechowywane dla potrzeb rozliczalności wraz z dokumentacją z obszaru ochrony danych osobowych.

B. Reguły bezpieczeństwa osobowego oraz teleinformatycznego

1. Placówka w ramach swojej działalności zapewnia bezpieczeństwo informacji, w szczególności w obszarze ich poufności, dostępności oraz integralności.
2. Wszystkie osoby dopuszczone w Placówce do przetwarzania danych są zobowiązane przejść wstępne szkolenie z zakresu ochrony danych oraz otrzymać upoważnienie do przetwarzania danych. Nadto osoby takie, wraz z upoważnieniem, potwierdzają zapoznanie się z dokumentacją ochrony danych oraz podpisują oświadczenie o zobowiązaniu się do zachowania poufności.
3. Pocztą elektroniczną należy przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed podsłuchem oraz przed przypadkowym rozproszeniem ich w Internecie.
4. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora sytemu. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora systemu oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.
5. Administrator systemu dobiera elektroniczne środki ochrony przed atakami z sieci, stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego i powiększania bazy danych.
6. Należy stosować następujące sposoby kryptograficznej ochrony danych:
    - przy dostępie do danych osobowych przez Internet używa się bezpiecznych stron HTTPS;
    - przy przesyłaniu danych osobowych przez pocztę elektroniczną należy je zaszyfrować, np. wstawiając do dokumentu Office (Word, Excel) i blokując dostęp do pliku przez ustanowienie hasła. Hasło powinno stać przekazane odbiorcy innym kanałem niż przesłany plik, np. przez SMS;

7. System informatyczny posiada szerokopasmowe połączenie z Internetem. Dostęp do niego jest ograniczony. Filtr treści (blokada niektórych kategorii stron) zapewnia Centrum Usług Informatycznych, konfigurowany zgodnie z wnioskiem dyrektora Placówki.

C. Zabezpieczenie sprzętu

1. W celu zapewnienia większego bezpieczeństwa i ochrony danych wykorzystywany jest system operacyjny Windows 10 i 11, posiadający rozbudowane mechanizmy nadawania uprawnień i praw dostępu.
2. Administrator systemu jest jedyną osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego. Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania ustalonych i statutowych zadań Placówki i posiadających ważną licencję użytkownika.
3. Bieżąca konserwacja sprzętu wykorzystywanego w Placówce do przetwarzania danych prowadzona jest przez administratora systemu.
4. Dopuszcza się konserwowanie i naprawę sprzętu poza Placówką po trwałym usunięciu danych lub na podstawie odrębnie podpisanej umowy powierzenia danych.
5. Zużyty sprzęt służący do przetwarzania danych, można zbyć dopiero po usunięciu danych, a urządzenia uszkodzone mogą być przekazywane do utylizacji dopiero po usunięciu danych.

D. Kontrola dostępu do systemu

1. Poszczególnym osobom upoważnionym do przetwarzania danych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator systemu po uprzednim zweryfikowaniu upoważnienia do przetwarzania danych, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.
2. Do zagwarantowania poufności i integralności danych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora systemu.

E. Zarządzanie ciągłością działania

1. Zapewnienie ciągłości działania Placówki w kontekście bezpieczeństwa informacji polega przede wszystkim na zapewnieniu dostępności informacji i narzędzi służących do jej przetwarzania.
2. Plany ciągłości działania Placówki, ze względu na charakter prowadzonej działalności edukacyjnej i społecznej, koncentrują się na:
    a. zapewnieniu dostępności infrastruktury informatycznej (łącza, serwery) oraz
    b. zapewnieniu dostępności usług informatycznych (w tym usług świadczonych przez firmy zewnętrzne, np. dostęp do Internetu, komunikacja między lokalizacjami, poczta elektroniczna i cloud computing).

Plany ciągłości działania w Placówce mają formę procedur postępowania wynikających z zawartych umów z dostawcami usług zewnętrznych, w szczególności z Centrum Usług Informatycznych oraz produktów zapewnianych przez Microsoft Corporation.

F. Zarządzanie dokumentacją SZBI

1. Za prawidłowe zarządzanie dokumentacją SZBI oraz za jej przechowywanie odpowiedzialny jest pracownik wyznaczony przez Dyrektora Placówki.

2. Zatwierdzona i podpisana dokumentacja SZBI przechowywana jest w formie papierowej w miejscu zabezpieczonym przed dostępem osób nieuprawnionych.
3. Polityka Ochrony Danych w wersji elektronicznej, z którą powinien zapoznać się ogół pracowników podlega publikacji wewnętrznymi kanałami. Każdy nowy pracownik powinien zostać zapoznany z tą dokumentacją przy okazji zatrudnienia; zatrudniany składa do akt osobowych oświadczenie o zapoznaniu się z Polityką Ochrony Danych i zobowiązuje się do jej przestrzegania.
4. Całość dokumentacji SZBI udostępniana jest nadto Dyrektorowi, upoważnionym pracownikom oraz IOD, którzy mają obowiązek się z nią zapoznać i odpowiednio stosować.
5. Każdy dokument składający się na SZBI powinien w swojej końcowej części zawierać adnotację dotyczącą wersji dokumentu. Każda zmiana w dokumencie SZBI powinna być odpowiednio dokumentowana poprzez dokonanie wpisu o nowej wersji, ze wskazaniem kolejnego numeru wersji, daty zmian, informacji o dokonanych zmianach oraz o autorze zmian.

G. Audytowanie systemu

System zarządzania bezpieczeństwem informacji (SZBI) - w szczególności Polityka Ochrony Danych, jak i wszelkie inne regulacje wewnętrzne dot. ochrony danych osobowych - powinien być poddawany przeglądowi przynajmniej raz na rok.

W razie istotnych zmian dotyczących przetwarzania danych osobowych Inspektor Ochrony Danych może zarządzić przegląd Polityki Ochrony Danych oraz pozostałej dokumentacji z zakresu ochrony danych, stosownie do potrzeb.

Inspektor Ochrony Danych przy współpracy z administratorem systemu analizuje, sprawdza czy SZBI jest adekwatny do:

- zmian w budowie systemu informatycznego,
- zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
- zmian w obowiązującym prawie.

Inspektor Ochrony Danych po uzgodnieniu z Dyrektorem Placówki może, stosownie do potrzeb, przeprowadzić audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu.

Dyrektor Placówki, biorąc pod uwagę wnioski Inspektora Ochrony Danych, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

H. Dokumenty powiązane

1) Procedura Zarządzania Bezpieczeństwem Systemów Informacyjnych
2) Procedura obiegu kluczy
3) Procedura nadawania upoważnień
4) Procedura – kontrola Urzędu Ochrony Danych
5) Procedura publikacji i aktualizacji danych w BIP
6) Procedura – placówka oświatowa jako podmiot przetwarzający
7) Procedura likwidacji kont pocztowych
8) Procedura - niszczenie dokumentów
9) Instrukcja reagowania na incydenty
10) Instrukcja postępowania w przypadku planowania procesu przetwarzania

11) Instrukcja spełniania obowiązku informacyjnego
12) Instrukcja bezpieczeństwa dla pracowników
13) Instrukcja bezpiecznej pracy dla odległość
14) Instrukcja nadawania haseł

Działając w imieniu Przedszkola nr 148 we Wrocławiu w dniu _____ r. przyjmuję niniejszą Politykę Ochrony Danych do stosowania wraz ze wszystkimi Załącznikami.

_____
Dyrektor Przedszkola nr 148 we Wrocławi