

POLITYKA BEZPIECZEŃSTWA
DANYCH OSOBOWYCH PRZETWARZANYCH W PRZEDSZKOLU
SAMORZĄDOWYM NR 60 W BIAŁYMSTOKU.

§ 1

1. Polityka bezpieczeństwa danych osobowych przetwarzanych w **Przedszkolu Samorządowym Nr 60 w Białymstoku** – zwana dalej Polityką bezpieczeństwa, **określa zasady przetwarzania danych osobowych w rozumieniu 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L119 s.1 z 2016 r., sprost. Dz. Urz. UE L127 s.2 z 2018 r., sprost. Dz. Urz. UE L74 s.35 z 2021 r.), zwanego dalej RODO.**
2. **Celem niniejszego dokumentu jest zapewnienie odpowiedniej ochrony danych osobowych i realizacji praw osób, których te dane dotyczą, poprzez zapewnienie zgodności z RODO oraz ustawą o ochronie danych osobowych z dnia 10 maja 2018 r.**
3. **Zasady określone w Polityce bezpieczeństwa obowiązują wszystkich pracowników Przedszkola Samorządowego Nr 60 w Białymstoku oraz inne osoby dopuszczone do przetwarzania danych osobowych na podstawie odrębnych umocowań prawnych.**
4. Polityka Bezpieczeństwa wraz z załącznikami ma wyłączoną jawność informacji i może być wykorzystywana tylko do celów służbowych, w tym do użytku przez pracowników **Przedszkola Samorządowego Nr 60 w Białymstoku** lub osoby upoważnione do przetwarzania danych osobowych oraz w celu zawarcia umowy powierzenia przetwarzania danych.

§ 2

Definicje

Użyte w dokumencie pojęcia oznaczają:

- 1) **Przedszkole** – **Przedszkole Samorządowe Nr 60 w Białymstoku;**
- 2) **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 (ogólne rozporządzenie o ochronie danych osobowych);
- 3) **dane osobowe** – są to wszelkie informacje o 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;
- 4) **przetwarzanie** – wszelkie operacje wykonywane na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;
 - 5) **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;
 - 6) **zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
 - 7) **administrator** (Administrator danych osobowych) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem jest Przedszkole, natomiast osobą reprezentującą Administratora jest Dyrektor Przedszkola;
 - 8) **podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
 - 9) **odbiorca** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Za odbiorców nie są uznawani pracownicy Administratora oraz organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego;
 - 10) **incydent bezpieczeństwa** – pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań Przedszkola i zagrażają bezpieczeństwu informacji; wykaz przykładowych zdarzeń stanowiących incydent bezpieczeństwa zawarty jest w **załączniku Nr 1** Polityki Bezpieczeństwa;
 - 11) **naruszenie ochrony danych osobowych** – oznacza incydent bezpieczeństwa prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

- 12) **szczególne kategorie danych osobowych** - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, dane dotyczące zdrowia fizycznego i psychicznego, orientacji seksualnej, dane genetyczne, dane biometryczne jednoznacznie identyfikujące osobę fizyczną (art. 9 pkt 1 RODO);
- 13) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych oraz sieć informatyczną zastosowanych w celu przetwarzania danych;

§ 3

Zarządzanie bezpieczeństwem i odpowiedzialność

1. Dyrektor Przedszkola decyduje o celach przetwarzania danych osobowych oraz zapewnia niezbędne środki do uzyskania zgodności modelu zarządzania bezpieczeństwem oraz stosowanych środków ochrony danych osobowych z przepisami określającymi zasady przetwarzania.
2. Dyrektor Przedszkola wyznaczył Inspektora Ochrony Danych (IOD), który realizuje zadania określone w art. 39 RODO, w tym:
 - 1) informuje Dyrektora Przedszkola, pracowników Przedszkola oraz podmioty przetwarzające o obowiązkach wynikających z Polityki bezpieczeństwa i doradza im w tej sprawie;
 - 2) monitoruje przestrzeganie realizacji Polityki bezpieczeństwa;
 - 3) zapewnia obsługę incydentów bezpieczeństwa;
 - 4) pełni rolę opiniodawczą w sprawach dotyczących przetwarzania danych osobowych.
3. Dyrektor Przedszkola zapewnia, aby IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, w tym informuje go o:
 - 1) zmianach w sposobie i zakresie przetwarzania danych osobowych;
 - 2) zakończeniu przetwarzania danych osobowych;
 - 3) każdym zleceniu realizacji zadania związanego z przetwarzaniem danych osobowych przez podmiot zewnętrzny;
 - 4) skardze na przetwarzanie danych osobowych;
 - 5) incydencie bezpieczeństwa.
4. Pracownik Przedszkola, zatrudniony przy przetwarzaniu danych osobowych, zobowiązany jest do:
 - 1) przestrzegania zasad Polityki bezpieczeństwa w trakcie realizacji zadań, które zostały mu powierzone do wykonania;
 - 2) przestrzegania **Zasad bezpieczeństwa przetwarzania informacji dla pracowników Przedszkola**, określonych odrębnym zarządzeniem;
 - 3) przetwarzania danych tylko na polecenie Dyrektora Przedszkola – przez **polecenie Dyrektora Przedszkola rozumie się zakres obowiązków pracownika lub inną formę**

udokumentowanego polecenia, w tym zarządzenie Dyrektora Przedszkola, a także w sytuacjach szczególnych polecenie ustne;

- 4) **niezwłocznego informowania Dyrektora Przedszkola o incydentach bezpieczeństwa;**
 - 5) **konsultowania z inspektorem danych osobowych wątpliwości dotyczących przetwarzania danych osobowych.**
5. Informatyk zatrudniony w Przedszkolu, administruje systemem informatycznym Przedszkola, zgodnie z dokumentem **Zasady zarządzania systemem informatycznym Przedszkola**, określonym odrębnym zarządzeniem.

§ 4

Zasady ogólne

1. Dane osobowe przetwarza się w Przedszkolu w celu realizacji zadań określonych przepisami prawa lub wynikających z przepisów prawa.
2. Przetwarzanie i ochrona danych osobowych podlega przepisom prawa, a w szczególności RODO. Zasada obowiązuje niezależnie od formy występowania danych, w tym formy papierowej lub elektronicznej oraz niezależnie od tego czy dane są uporządkowane (zbiory danych, zestawienia, rejestry) lub nieuporządkowane (notatki, pisma).
3. Przetwarzanie danych osobowych w Przedszkolu odbywa się w formie papierowej lub elektronicznej, w systemach informatycznych, w zbiorach danych osobowych, a także poza nimi.
4. Dane osobowe przetwarza się w Przedszkolu przy zachowaniu zasad RODO, a w szczególności dane osobowe muszą być:
 - 1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
 - 2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami („ograniczenie celu”);
 - 3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
 - 4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
 - 5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do

celów statystycznych, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

- 6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).
5. Przetwarzanie danych osobowych odbywa się z zapewnieniem dbałości o możliwość wykazania przestrzegania zasad wskazanych w ustępie poprzednim, w szczególności poprzez dokumentowanie („rozliczalność”).

§ 5

Przetwarzanie danych osobowych przez zatrudnione osoby

1. **Wszystkie osoby dopuszczone do przetwarzania danych osobowych lub dopuszczone do systemu informatycznego, zostają zapoznane z Polityką bezpieczeństwa i zobowiązane są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania – zarówno w trakcie, jak i po ustaniu zatrudnienia.** Fakt ten potwierdzają stosownym oświadczeniem, stanowiącym **załącznik Nr 2** Polityki Bezpieczeństwa.
2. Każda osoba dopuszczona do przetwarzania zobowiązana jest do uczestniczenia w szkoleniach z zakresu bezpieczeństwa i ochrony danych osobowych. Potwierdzeniem odbycia przedmiotowego szkolenia jest zaświadczenie o odbyciu szkolenia.
3. **Dostęp do danych osobowych odbywa się na podstawie upoważnienia** wydanego przez Administratora i w zakresie wydanego przez niego polecenia.
4. Upoważnienia do przetwarzania danych osobowych wydawane są zgodnie z brzmieniem określonym w **załączniku Nr 3**, w przypadku pracowników Przedszkola jak i osób nie będących pracownikami (tj. stażysty, wolontariusze, praktykanci, aplikanci, zleceniobiorcy).
5. Upoważnienia do przetwarzania danych osobowych są nadawane:
 - 1) na czas nieokreślony w sytuacji, gdy dotyczą zadań realizowanych stale i czas zakończenia ich realizacji w momencie udzielania upoważnienia nie jest znany;
 - 2) na czas określony w sytuacji, gdy dotyczą zadań realizowanych w określonym przedziale czasu wynikającym np. z umowy, realizowanego projektu, pracy zespołu roboczego.
6. W przypadku powierzenia przetwarzania danych podmiotowi przetwarzającemu, podmiot ten wydaje upoważnienia pracownikom własnym lub dokonuje dalszego powierzenia przetwarzania danych na zasadach określonych w umowie powierzenia przetwarzania danych.

7. Przetwarzanie danych osobowych, w tym kopiowanie danych osobowych oraz wykonywanie wydruków z danych elektronicznych może wynikać z potrzeb realizacji zadań służbowych oraz może być realizowane w ramach kompetencji, przy zachowaniu zasad określonych w dokumencie **Zasady bezpieczeństwa przetwarzania informacji dla pracowników Przedszkola.**

§ 6

Zgłaszanie incydentów bezpieczeństwa i naruszeń ochrony danych osobowych

1. **Pracownik Przedszkola, który wykrył incydent bezpieczeństwa, uczestniczył w nim lub doprowadził do niego, zobowiązany jest do niezwłocznego zawiadomienia o tym fakcie Dyrektora Przedszkola, a w przypadku jego nieobecności osobę zastępującą Dyrektora Przedszkola.**
2. Dyrektor Przedszkola podejmuje decyzję o zgłoszeniu incydentu bezpieczeństwa IOD.
3. IOD, po zgłoszeniu do niego incydentu bezpieczeństwa:
 - 1) dokonuje rejestracji incydentu bezpieczeństwa w rejestrze incydentów bezpieczeństwa;
 - 2) dokonuje oceny, czy incydent bezpieczeństwa stanowi naruszenie ochrony danych osobowych, czy wymagane jest zgłoszenie go Prezesowi Urzędu Ochrony Danych Osobowych i przekazuje swoje ustalenia Dyrektorowi Przedszkola;
 - 3) dokonuje oceny, czy wymagane jest poinformowanie osób, których naruszenie dotknęło i przekazuje swoje ustalenia Dyrektorowi Przedszkola;
 - 4) po uzyskaniu zgody od Dyrektora Przedszkola, przygotowuje projekt zgłoszenia naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych, na podstawie informacji uzyskanych z Przedszkola;
 - 5) we współpracy z wyznaczonym pracownikiem Przedszkola przygotowuje projekt zawiadomienia osób o naruszeniu ochrony ich danych osobowych, o ile takie zawiadomienie jest konieczne.
4. W przypadku naruszenia ochrony danych osobowych, Dyrektor Przedszkola jest zobowiązany do:
 - 1) dokonania zgłoszenia tego naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, w terminie nie dłuższym niż 72 godziny po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw i wolności osób fizycznych; zgłoszenia dokonuje się na formularzu i zgodnie z wytycznymi zamieszczonymi na stronie internetowej Prezesa Urzędu Ochrony Danych Osobowych;
 - 2) zawiadomienia o tym fakcie osoby, której dane dotyczą, bez zbędnej zwłoki, jeżeli naruszenie ochrony danych może powodować wysokie ryzyko naruszenia praw i wolności.
5. Dyrektor Przedszkola dokonuje zgłoszenia naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych, zgodnie z projektem zawiadomienia przygotowanym przez IOD, o ile takie zawiadomienie jest konieczne.

6. Dyrektor Przedszkola dokonuje zawiadomienia osób o naruszeniu ich danych osobowych, zgodnie z projektem zawiadomienia przygotowanym przez IOD, o ile takie zawiadomienie jest konieczne.

§ 7

Realizacja obowiązku informacyjnego

1. Każdej osobie, której dane przetwarzane są przez Przedszkole, należy w zwięzłej i zrozumiałej formie przedstawić informacje o przetwarzaniu jej danych.
2. Informacje przekazywane są w postaci klauzul informacyjnych zawierających niezbędne elementy, wskazane w przepisach.
3. Każdy pracownik Przedszkola zobowiązany jest stosować klauzule informacyjne w niniejszych przypadkach:
 - 1) w przypadku zbierania danych osobowych bezpośrednio od osoby, której one dotyczą (art. 13 RODO) – informacje zawarte w klauzuli informacyjnej należy przedstawić nie później niż w momencie pozyskiwania danych.
 - 2) w przypadku pozyskiwania danych osobowych, w sposób inny niż od osoby, której dotyczą (art. 14 RODO) – informacje zawarte w klauzuli informacyjnej należy przedstawić osobie, której dane osobowe dotyczą:
 - a) w rozsądnym terminie po uzyskaniu danych osobowych – najpóźniej w ciągu miesiąca,
 - b) jeżeli dane osobowe mają być stosowane w komunikacji z osobą, której dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą,
 - c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy pierwszym ujawnieniu.
4. Stosowanie klauzul nie obowiązuje w przypadkach:
 - 1) gdy osoba, której dane osobowe dotyczą dysponuje już tymi informacjami;
 - 2) zbierania danych osobowych, w inny sposób niż od osoby której dotyczą i:
 - a) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby to niewspółmiernie dużego wysiłku,
 - b) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane przepisami prawa, przewidującymi odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą,
 - c) dane muszą pozostawać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianej przepisami prawa, w tym ustawowym obowiązkiem zachowania tajemnicy.
5. Wzory klauzul informacyjnych (przed rozpoczęciem stosowania) oraz decyzję o niestosowaniu klauzuli informacyjnej należy skonsultować z IOD.

§ 8

Realizacja praw osoby, której dane dotyczą

1. Osobie, której dane przetwarza Przedszkole przysługuje:

- 1) prawo dostępu do danych, o którym mowa w art. 15 RODO. Prawo to zapewnia osobie, której dane dotyczą, uzyskanie od Administratora potwierdzenia, czy jej dane są przetwarzane, a jeżeli ma to miejsce, zapewnia uzyskanie dostępu do nich oraz do następujących informacji:
 - a) cele przetwarzania,
 - b) kategorie odnośnych danych osobowych,
 - c) informacje o odbiorcach lub kategoriach odbiorców danych, którym dane zostały lub zostaną udostępnione,
 - d) planowany okres przechowywania danych lub kryteria ustalenia tego okresu,
 - e) informacje o innych przysługujących jej uprawnieniach, włącznie z prawem do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,
 - f) informacje o źródle pochodzenia danych, jeżeli dane zostały zebrane od osób trzecich,
 - g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu,
 - h) jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną. Prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych.

- 2) prawo do sprostowania danych, w przypadku jeżeli są nieprawidłowe lub niekompletne. Szczegółowe zasady zostały określone w **załączniku Nr 4** do Polityki bezpieczeństwa (pkt 1).
- 3) prawo do usunięcia danych („prawo do bycia zapomnianym”) przysługuje w szczególności w przypadku, jeżeli:
 - a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane,
 - b) osoba, której dane dotyczą cofnęła zgodę na ich przetwarzanie, a przetwarzanie opierało się na zgodzie tej osoby,
 - c) osoba, której dane dotyczą wnosi sprzeciw wobec przetwarzania danych (prawo wskazane w pkt 6), który jest rozpatrzony pozytywnie,
 - d) dane były przetwarzane niezgodnie z prawem,
 - e) dane muszą być usunięte w celu wywiązania się z obowiązków określonych przepisami prawa,
 - f) dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Szczegółowe zasady zostały określone w **załączniku Nr 4** do Polityki bezpieczeństwa (pkt 2).

- 4) prawo do ograniczenia przetwarzania polegające na ograniczeniu przetwarzania do przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Prawo to przysługuje jeżeli:
- a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych,
 - b) przetwarzanie jest niezgodne z prawem, a osoba której dane dotyczą sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
 - c) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dotyczą, do ustalenia, dochodzenia, lub obrony roszczeń,
 - d) osoba, której dane dotyczą, wniosła sprzeciw (prawo wskazane w pkt 6), do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec sprzeciwu osoby, której dane dotyczą.

Szczegółowe zasady zostały określone w **załączniku Nr 4** do Polityki bezpieczeństwa (pkt 3).

- 5) prawo do przenoszenia danych, zapewniające osobie, której dane dotyczą, otrzymanie w ustrukturyzowanym, powszechnie używanym formacie danych osobowych jej dotyczących, które dostarczyła Administratorowi, w tym przesłanie tych danych innemu Administratorowi. Prawo realizuje się w przypadku gdy przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, lub gdy jest niezbędne do wykonania umowy lub podjęcia działań na żądanie osoby przed zawarciem umowy, lub gdy przetwarzanie odbywa się w sposób zautomatyzowany. Szczegółowe zasady zostały określone w **załączniku Nr 4** do Polityki bezpieczeństwa (pkt 4).
- 6) prawo do sprzeciwu wobec przetwarzania danych jej dotyczących, skutkujące obowiązkiem zaprzestania przetwarzania danych osobowych, przysługujące:
- a) z przyczyn związanych z jej szczególną sytuacją, wobec przetwarzania opartego o przesłanki zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej lub przetwarzania niezbędnego do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub stronę trzecią,
 - b) w przypadku przetwarzania na potrzeby marketingu bezpośredniego.

Szczegółowe zasady zostały określone w **załączniku Nr 4** do Polityki bezpieczeństwa (pkt 5).

- 7) prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu. Szczegółowe zasady zostały określone w **załączniku Nr 4** do Polityki bezpieczeństwa (pkt 6)

2. Realizacja praw wskazanych w ustępie poprzednim następuje **bez zbędnej zwłoki** – a w każdym razie w **terminie miesiąca** od otrzymania żądania – należy udzielić osobie informacji o działaniach podjętych w związku z realizacją żądań wynikających z tych praw. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. Wówczas w terminie miesiąca od otrzymania żądania należy poinformować osobę o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeżeli nie są i nie będą podejmowane działania w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania należy poinformować osobę o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz skorzystania ze środków ochrony prawnej przed sądem.
3. Dyrektor Przedszkola realizujący prawa osób, wskazane w niniejszym paragrafie, jest zobowiązany poinformować o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Dyrektor Przedszkola informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą tego zażąda.
4. Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz wykonywaniem praw przysługujących im na mocy RODO.

§ 9

Udostępnienie danych

1. Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, mogą wnosić o udostępnienie (ujawnienie im) danych osobowych, przy czym zakres danych powinien być określony. Udostępnienie następuje w celu wskazanym przez wnioskującego, w sytuacjach określonych w przepisach prawa. Szczegółowa procedura udostępnienia danych została określona w dokumencie Procedura udostępniania danych osobowych, stanowiącym **załącznik Nr 5** do Polityki bezpieczeństwa.
2. Decyzję o udostępnieniu danych podejmuje Dyrektor Przedszkola, który odpowiada za poprawność merytoryczną danych. Dyrektor Przedszkola może delegować wyznaczonym pracownikom, których nadzoruje, prawo do podejmowania decyzji o udostępnieniu danych, w przypadku dostępu stron lub ich pełnomocników do akt sprawy.
3. IOD doradza w zakresie udostępniania danych osobowych.
4. Udostępnianie danych za pośrednictwem systemu informatycznego musi być poprzedzone projektowaniem przetwarzania danych osobowych, o którym mowa w § 14.

§ 10

Powierzenie przetwarzania danych osobowych

1. Jeżeli przetwarzanie danych osobowych odbywa się w imieniu Administratora przez inny podmiot, to warunkiem tego przetwarzania jest zawarcie umowy powierzenia przetwarzania tych danych, nie później niż w momencie rozpoczęcia tego przetwarzania, chyba że przetwarzanie to odbywa się na podstawie innego instrumentu prawnego.
2. Projekt umowy powierzenia przetwarzania danych osobowych należy skonsultować z IOD.
3. Umowę powierzenia przetwarzania danych osobowych zawiera Dyrektor Przedszkola.
4. Dyrektor Przedszkola informuje IOD o zawarciu umowy powierzenia przetwarzania danych osobowych i o jej wygaśnięciu, celem dokonania wpisu do rejestru czynności przetwarzania danych, o którym mowa w § 13.

§ 11

Retencja – usuwanie danych po czasie

1. Stosowanie zasady „ograniczenia przechowywania” wymaga usunięcia danych osobowych po osiągnięciu celu lub celów przetwarzania.
2. Termin osiągnięcia celu może wynikać w szczególności z:
 - 1) przepisów prawa;
 - 2) terminu realizacji umowy;
 - 3) terminu realizacji projektu lub zadania;
 - 4) ustaleń, w oparciu o uzasadnione praktyczne przesłanki wskazujące na celowość przetwarzania danych.
3. Za nadzór nad stosowaniem zasady „ograniczenia przechowywania” odpowiada Dyrektor Przedszkola, w tym:
 - 1) ustala termin osiągnięcia celu;
 - 2) nadzoruje czas przechowywania dokumentacji papierowej;
 - 3) nadzoruje czas przechowywania danych elektronicznych w systemach informatycznych, w tym poczty elektronicznej;
 - 4) nadzoruje pracowników pod kątem przechowywania przez nich dokumentacji roboczej, w tym plików z elektronicznymi wersjami dokumentów oraz różnego rodzaju zestawień tych danych;
 - 5) podejmuje działania celem terminowego usuwania dokumentacji papierowej i elektronicznej oraz danych elektronicznych;

§ 12

Analiza ryzyka naruszenia praw i wolności osób fizycznych

1. Analiza ryzyka naruszenia praw i wolności osób fizycznych jest przeprowadzana w sytuacjach:

- 1) w trakcie planowania przetwarzania danych osobowych, jeszcze przed rozpoczęciem ich przetwarzania lub przed każdą istotną zmianą w przetwarzaniu danych osobowych, w ramach projektowania przetwarzania danych, o którym mowa w §14;
 - 2) okresowo, stosownie do zmian w otoczeniu prawnym, technicznym i organizacyjnym – potrzebę przeprowadzenia okresowej analizy ryzyka monitoruje IOD;
 - 3) każdorazowo w przypadku zaistnienia naruszenia ochrony danych osobowych.
2. Dyrektor Przedszkola, przy wsparciu ustalonego przez siebie zespołu pracowników, dokonuje analizy ryzyka naruszenia praw i wolności osób fizycznych, w obszarze działalności nadzorowanej przez niego jednostki organizacyjnej.
 3. IOD doradza w zakresie przeprowadzania analizy ryzyka.
 4. Analiza ryzyka naruszenia praw i wolności osób fizycznych jest przeprowadzana w sytuacjach:
 - 1) w trakcie planowania przetwarzania danych osobowych, jeszcze przed rozpoczęciem ich przetwarzania lub przed każdą istotną zmianą w przetwarzaniu danych osobowych, w ramach projektowania przetwarzania danych, o którym mowa w §14;
 - 2) okresowo, stosownie do zmian w otoczeniu prawnym, technicznym i organizacyjnym – potrzebę przeprowadzenia okresowej analizy ryzyka monitoruje IOD;
 - 3) każdorazowo w przypadku zaistnienia naruszenia ochrony danych osobowych – analizę ryzyka naruszenia praw i wolności osób wykonuje IOD, zgodnie z metodą ENISA.
 5. Analiza ryzyka jest przeprowadzana zgodnie z dokumentem „*Metodyka analizy ryzyka naruszenia praw i wolności osób fizycznych*” stanowiącym **załącznik Nr 6** do Polityki bezpieczeństwa.

§ 13

Rejestrowanie czynności przetwarzania

1. Rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora, w imieniu Dyrektora Przedszkola prowadzi IOD. W rejestrach muszą być wykazane wszystkie czynności przetwarzania (procesy, w których są wykonywane operacje na danych osobowych) wraz z wymaganymi o nich informacjami.
2. Rejestry wskazane w ust. 1 mają formę pisemną, w tym formę elektroniczną.
3. Rejestr czynności przetwarzania danych osobowych zawiera co najmniej informacje:
 - 1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
 - 2) cele przetwarzania;
 - 3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
 - 4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

- 5) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej;
 - 6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
4. Rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora zawiera co najmniej informacje:
- 1) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
 - 2) kategorie przetwarzania dokonywanych w imieniu każdego z administratorów;
 - 3) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej;
 - 4) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

§ 14

Projektowanie przetwarzania danych osobowych

1. Przed przystąpieniem do przetwarzania danych osobowych lub przed zmianą w sposobie lub zakresie przetwarzania danych osobowych, należy zaprojektować proces przetwarzania danych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych. Projektowanie przetwarzania obejmuje określenie i udokumentowanie:
 - 1) celów przetwarzania danych, w ramach zdefiniowanych czynności przetwarzania, o których mowa w §13;
 - 2) operacji przetwarzania danych tj. czynności technicznych na danych;
 - 3) zakresu danych niezbędnych do funkcjonowania projektowanego procesu przetwarzania danych;
 - 4) zasobów niezbędnych do funkcjonowania procesu przetwarzania danych;
 - 5) ryzyk naruszenia praw i wolności osób fizycznych dla poszczególnych operacji przetwarzania danych, w tym ryzyk bezpieczeństwa danych osobowych, zgodnie z §12;
 - 6) domyślnych środków technicznych i organizacyjnych ochrony danych osobowych;
 - 7) osób odpowiedzialnych za nadzór nad wprowadzeniem środków ochrony danych osobowych;
2. Jeżeli analiza ryzyk naruszenia praw i wolności osób fizycznych wykaże, że dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, to projektowanie przetwarzania danych osobowych rozszerza się o

dokonanie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, która zawiera co najmniej:

- 1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
 - 2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
 - 3) ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą;
 - 4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
3. Jeżeli ocena skutków dla ochrony danych osobowych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby nie zostały zastosowane środki w celu zminimalizowania tego ryzyka, to projektowanie przetwarzania danych osobowych rozszerza się o konsultację z Prezesem Urzędu Ochrony Danych Osobowych, przedstawiając mu:
- 1) gdy ma to zastosowanie – odpowiednie obowiązki Administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu;
 - 2) cele i sposoby zamierzonego przetwarzania;
 - 3) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z RODO;
 - 4) dane kontaktowe IOD;
 - 5) ocenę skutków dla ochrony danych, o której mowa w ustępie poprzednim;
 - 6) wszelkie informacje, których zarządza Prezes Urzędu Ochrony Danych Osobowych.
4. Dyrektor Przedszkola, odpowiada za:
- 1) zaprojektowanie przetwarzania danych osobowych przed rozpoczęciem przetwarzania tych danych;
 - 2) uzyskanie pozytywnej opinii IOD w zakresie projektu przetwarzania danych osobowych, w tym jeżeli wystąpi taka konieczność, skonsultowanie i uzyskanie pozytywnej opinii IOD w zakresie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych;
 - 3) przekazywanie do IOD niezbędnych informacji w procesie projektowania przetwarzania danych osobowych.
5. Z uwagi na skomplikowany charakter projektowania przetwarzania danych osobowych, w tym oceny skutków dla przetwarzania danych osobowych, IOD wspiera Dyrektora Przedszkola w całości procesu projektowania przetwarzania danych, a w szczególności:
- 1) określa i udostępnia wzory niezbędnej dokumentacji;
 - 2) udziela konsultacji dotyczących projektowania przetwarzania danych;

- 3) informuje Dyrektora Przedszkola o konieczności przeprowadzenia oceny skutków przetwarzania dla ochrony danych osobowych;
 - 4) przygotowuje projekt dokumentu oceny skutków przetwarzania dla ochrony danych osobowych, po zgłoszeniu przez Dyrektora Przedszkola takiej potrzeby i otrzymaniu od niego niezbędnych informacji;
 - 5) informuje Dyrektora Przedszkola o niezbędnej dokumentacji do konsultacji z Prezesem Urzędu Ochrony Danych Osobowych;
 - 6) odpowiada za komunikację z Prezesem Urzędu Ochrony Danych Osobowych.
6. Zmiana lub dodanie operacji przetwarzania do wcześniej zaprojektowanego procesu przetwarzania danych osobowych wymaga przeprowadzenia projektowania przetwarzania danych osobowych. IOD podejmuje decyzję, czy projektowanie przetwarzania odbędzie się dla całości procesu, czy tylko dla zmienionej lub dodanej operacji przetwarzania i informuje o tym fakcie Dyrektora Przedszkola.

§ 15

Postanowienia końcowe

1. Żadne odstępstwa od zasad bezpieczeństwa ustalone w Polityce bezpieczeństwa nie są dopuszczalne bez uzyskania zgody Dyrektora Przedszkola.
2. **Naruszenie zasad określonych w Polityce bezpieczeństwa stanowić będzie podstawę do odpowiedzialności dyscyplinarnej lub karnej.**