Załącznik do Zarządzenia Dyrektora

Przedszkola „Kraina Marzeń”

w Czarnej Białostockiej z dnia 23.05.2018r. w sprawie dokumentacji

ochrony danych osobowych RODO

tekst ujednolicony 29.09.2020r.- zmiana zał. 13

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

w Przedszkolu " Kraina Marzeń"

w Czarnej Białostockiej

(nazwa podmiotu)

ul. Torowa 26, 16-020 Czarna Białostocka

ROZDZIAŁ 1
Postanowienia ogólne

§ 1. Celem Polityki Bezpieczeństwa Przetwarzania Danych Osobowych zwana dalej „Polityką bezpieczeństwa", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2. Polityka bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z 10 maja 2018r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000) oraz 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 95/49/WE. W razie zmiany obowiązujących przepisów prawa powodujących niezgodność niniejszego dokumentu z nimi, Polityka bezpieczeństwa zostanie dostosowana do obowiązujących przepisów.

§ 3. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

ROZDZIAŁ 2
Definicje

§ 4. Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1. **Administrator danych osobowych –**rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę decydującą o celach i środkach przetwarzania danych osobowych;
2. **Inspektor ochrony danych** – rozumie się przez to osobę wyznaczoną przez administratora danych osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
3. **Ustawa o ochronie danych osobowych**– rozumie się przez to ustawę z 10 maja 2018r. o ochronie danych osobowych
4. **Rozporządzenie** – 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 95/49/WE.
5. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
6. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
7. **Przetwarzanie danych –** rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
8. **System informatyczny –** rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
9. **System tradycyjny** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
10. **Zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

11. **Administrator systemu informatycznego** – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi;
12. **Użytkownik** – rozumie się przez to upoważnionego przez administratora danych osobowych wyznaczonego do przetwarzania danych osobowych pracownika;
13. **Identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
14. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

ROZDZIAŁ 3
Zakres i cel stosowania

§ 5. 1. Administrator danych osobowych to:

Przedszkole " Kraina Marzeń" w Czarnej Białostockiej
Osobą administrującą w imieniu podmiotu jest: ***Danuta Kowalewska***

2. Zgodnie z art. 37 Rozporządzenia Administrator powołuje **Inspektora ochrony danych,** którym jest:

1) Imię i nazwisko : Rafał Andrzejewski
2) E-mail kontaktowy: **and1rafal@go2.pl**
3) Dane Inspektora Ochrony Danych Osobowych udostępniono na stronie internetowej: **http://www. kraina-marzen.przyjdz.com**

3. Inspektor ochrony danych realizuje zadania w zakresie nadzoru nad przestrzeganiem ochrony danych osobowych, w tym zwłaszcza:

1) informuje administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy rozporządzenia Parlamentu europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95 /46/WE, zwanego dalej rozporządzeniem oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) monitoruje przestrzeganie rozporządzenia, innych przepisów Unii państw członkowskich o ochronie danych osobowych oraz polityki administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania, zgodnie z art. 35 rozporządzenia;
4) współpracuje z organem nadzorczym;
5) pełnieni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia oraz w stosownych przypadkach prowadzi konsultacji we wszystkich innych sprawach

§ 6. 1. Celem Polityki bezpieczeństwa jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.

2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1) **poufność danych** – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
2) **integralność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3) **rozliczalność danych** – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
4) **integralność systemu** – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
5) **dostępność informacji** – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;

3. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych, **zarządzanie ryzykiem** rozumiane jest jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 7. 1. Zapisy polityki bezpieczeństwa zobowiązane są stosować wszystkie osoby, które w podmiocie mają dostęp do danych osobowych.

2. Polityka bezpieczeństwa dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (system tradycyjny, systemy informatyczne).

3. Polityka bezpieczeństwa ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.

§ 8. Politykę bezpieczeństwa stosuje się w szczególności do:

1) danych osobowych przetwarzanych w systemach informatycznych;
2) wszystkich informacji dotyczących danych osobowych zawartych w przetwarzanych zbiorach;
3) wszystkich lokalizacji – budynków i pomieszczeń, w których są przetwarzane dane (wykaz miejsc przetwarzania danych stanowi ***zał.nr 1*** do niniejszej Polityki bezpieczeństwa);
4) wszystkich informacji danych zawartych w opisie struktury zbiorów;
5) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;
6) rejestru osób upoważnionych do przetwarzania danych osobowych;
7) innych dokumentów zawierających dane osobowe.

§ 9.1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki bezpieczeństwa mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
3) wszystkich pracowników, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez dokumenty Polityki bezpieczeństwa zobowiązani są wszyscy pracownicy, w tym inne osoby mające dostęp do informacji podlegających ochronie.

ROZDZIAŁ 4
Zbiory danych osobowych

§ 10. Dane osobowe gromadzone są w zbiorach danych. Wykaz zbiorów danych wraz ze wskazaniem systemu informatycznego służącego do przetwarzania danych stanowi ***zał. nr 2*** do niniejszej Polityki bezpieczeństwa.

§ 11. Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych **i p**rzepływ danych pomiędzy poszczególnymi systemami został określony w ***zał. nr 3*** do niniejszej Polityki bezpieczeństwa.

ROZDZIAŁ 5
Nadawanie upoważnień do przetwarzania danych osobowych

§ 12. 1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych osobowych. Wykaz osób upoważnionych do przetwarzania danych osobowych stanowi ***zał. nr 4*** *, a wz*ór upoważnienia stanowi ***zał. nr 5*** do niniejszej Polityki bezpieczeństwa.
2. Administrator danych osobowych nadając uprawnienia pracownikom, którzy przetwarzają dane odbiera od pracownika oświadczenie o zachowaniu danych w poufności oraz o zapoznaniu się z dokumentami określającymi zasady zabezpieczania i przetwarzania danych osobowych w podmiocie. ***zał. nr 6***
3. Administrator danych osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która stanowi ***zał. nr 7*** do niniejszej Polityki bezpieczeństwa.

ROZDZIAŁ 6
Udostępnienie i powierzanie danych osobowych

§ 13. 1. Administrator danych osobowych bądź pracownicy upoważnieni do przetwarzania danych mogą udostępnić dane osobie wnioskującej z zachowaniem zasady, że udostępnienie danych osobowych nie może naruszać praw i wolności osoby, których dane dotyczą. Wzór wniosku o udostępnienie danych stanowi ***zał. nr 9*** do niniejszej Polityki bezpieczeństwa. Każdorazowe udostępnienie danych musi być odnotowane w rejestrze udostępnienia, który stanowi ***zał. nr 10*** do niniejszej Polityki bezpieczeństwa.
2. Dopuszczalne jest powierzenie przez administratora danych przetwarzania danych podmiotom zewnętrznym.
3. Powierzenie przetwarzania danych może mieć miejsce na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać też zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy oraz sposób rozwiązania umowy. Wzór umowy powierzenia danych stanowi ***zał. nr 8*** do niniejszej Polityki bezpieczeństwa.
4. Powierzenie przetwarzania danych osobowych musi uwzględniać ponadto wymogi określone w Rozporządzeniu. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia odpowiednich środków zabezpieczających zbiór danych.
5. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności administratora danych za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa administratora danych do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki bezpieczeństwa, Instrukcji zarządzania systemem informatycznym oraz właściwych przepisów prawa.
6. Wykaz podmiotów, którym powierzono przetwarzanie danych stanowi ***zał. nr 11*** do niniejszej Polityki bezpieczeństwa.

7. Powierzenie przetwarzania danych uregulowane w Polityce bezpieczeństwa nie ma zastosowania do przekazywania danych podmiotom upoważnionym do ich przetwarzania na mocy przepisów prawa, w tym w szczególności ZUS, Prokuraturze, Policji, Sądom, Komornikom, itd.

ROZDZIAŁ 7
Wynoszenie akt i dokumentacji

§ 14. 1. Poza miejsca przetwarzania danych wskazanych **w *zał. nr 1*** nie wolno wynosić żadnej dokumentacji ani akt związanych z wykonywaniem czynności służbowych, a zwłaszcza dokumentów zawierających dane osobowe.
2. Przepis powyższy nie dotyczy tych pracowników, których zakres obowiązków wymaga dokonywania czynności służbowych z dokumentacją zawierającą dane osobowe poza obszarem przetwarzania danych, a także czynności związanych z przesyłaniem i transportem korespondencji.
3. Pracownicy, o których mowa w punkcie powyżej, są zobowiązani stosować środki zapewniające ochronę powierzonych danych osobowych podczas ich transportu, przechowywania i użytkowania poza obszarem siedziby pracodawcy, a w szczególności zabezpieczyć te dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Rozporządzenia i Ustawy o ochronie danych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Pracownicy tacy ponoszą pełną odpowiedzialność za powierzony im sprzęt oraz dokumentację znajdującą się poza siedzibą administratora.
5. Każdy pracownik, który podejrzewa, iż mogło nastąpić naruszenie bezpieczeństwa ochrony danych osobowych lub próba dokonania takiego naruszenia przez osoby nieupoważnione, jest zobowiązany do niezwłocznego poinformowania o powyższym administratora danych osobowych, który prowadzi postępowanie kontrolne, pod kątem wyjaśnienia okoliczności ewentualnego naruszenia bezpieczeństwa danych osobowych.
6. Odpowiedzialność za bezpieczeństwo dokumentacji lub akt wynoszonych poza obszar przetwarzania danych ponosi pracownik, który te akta wynosi, z chwilą ich pobrania. Odpowiedzialność ta dotyczy również danych znajdujących się na nośnikach cyfrowych.
7. Po zwrocie akt i dokumentacji (lub przenośnych komputerów) przez pracownika, przełożony zobowiązany jest do jej sprawdzenia pod kątem zgodności ze stanem sprzed wypożyczenia.
8. Pozostawanie w pracy po godzinach pracy może mieć miejsce tylko w związku z pełnionymi obowiązkami i za zgodą administratora danych lub osoby przez niego upoważnionej.
9. Każdy pracownik po zakończeniu pracy zobowiązany jest zamknąć w szafach wszelką dokumentację oraz komputer przenośny (w przypadku jego używania), a następnie osobiście zabezpieczyć klucze z zachowaniem wszelkich zasad bezpieczeństwa. Instrukcję w sprawie określenia procedury postępowania z kluczami stanowi z***ał. Nr 13*** do Polityki bezpieczeństwa.

ROZDZIAŁ 8
Zasady korzystania z komputerów przenośnych

§ 15.1. Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków.
2. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie za zgodą administratora danych lub osoby przez niego upoważnionej.
3. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala bezpośredni przełożony pracownika za wiedzą administratora danych.
4. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

§ 16. Użytkownik komputera przenośnego zobowiązany jest do:

1) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności: transportowania komputera w bagażu podręcznym, nie pozostawiania komputera w samochodzie, przechowalni bagażu, itp.,
2) przenoszenia komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych,
3) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
4) nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,
5) zabezpieczania komputera przenośnego hasłem i blokowanie dostępu przed użyciem przez osoby postronne,
6) kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych,
7) umożliwienia, poprzez podłączenie komputera do sieci informatycznej administratora danych w celu aktualizacji wzorców wirusów w programie antywirusowym,
8) utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł,
9) wykorzystywania haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
10) zmiany haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ 9
Środki techniczne i organizacyjne zabezpieczenia danych osobowych

§ 17. 1. Zabezpieczenia organizacyjne:
1) sporządzono i wdrożono Politykę bezpieczeństwa;
2) wyznaczono inspektora ochrony danych
3) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
4) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych, bądź osobę przez niego upoważnioną;
5) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
6) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
7) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
8) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
9) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
10) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
11) wprowadzono zasadę „czystego biurka" i „białej kartki";
12) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób;
13) informacji telefonicznych nie udziela się, względnie udziela się po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych;
14) wdrożono procedurę nadzoru nad naruszeniami „rejestr naruszeń"

2. Zabezpieczenia techniczne:

1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci
2) publicznej za pomocą zapory firewall
3) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową;
4) konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem używanych aplikacji;
5) zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika;
6) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła;

3. Zakres zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej stanowi Instrukcja zarządzania systemem informatycznym ***zał. Nr 14***

4. Środki ochrony fizycznej:
1) urządzenia służące do przetwarzania danych osobowych i dokumentację zawierającą dane osobowe umieszcza się w zamykanych pomieszczeniach;
2) obszar, w którym przetwarzane są dane osobowe, chroniony jest poprzez zastosowanie: pomieszczenia zamykane na klucz, kraty w oknach.

ROZDZIAŁ 10
Szkolenia użytkowników

§ 18.1. Każdy użytkownik przed dopuszczeniem do pracy w systemie tradycyjnym i systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej zostaje poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

2. Za zorganizowanie szkolenia odpowiada administrator danych osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami Rozporządzenia, Ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u administratora danych osobowych.
4. Zgodnie z wymogami Ustawy o ochronie danych pracownicy zostają zapoznani z przepisami z zakresu ochrony danych osobowych w każdym przypadku istotnych zmian w przepisach dotyczących przetwarzania danych.
5. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
6. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ 11
Postanowienia końcowe

§ 19. 1. Wszyscy pracownicy zobowiązani są do zapoznania się z niniejszym dokumentem oraz do stosowania zawartych w nim reguł.

2. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

3. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z Ustawą o ochronie danych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
4. W sprawach nieuregulowanych w polityce mają zastosowanie przepisy Rozporządzenia oraz Ustawy o ochronie danych osobowych.
5. Dokumentami powiązanymi z niniejszą polityką są:
Instrukcja zarządzania systemem informatycznym, Regulamin poczty elektronicznej, Instrukcja w sprawie określenia procedury postępowania z kluczami.
6. Integralną część dokumentacji stanowią załączniki:

- Zał. Nr 1 Wykaz budynków i pomieszczeń
- Zał. Nr 2 Wykaz zbiorów danych ze wskazaniem systemów do ich przetwarzani
- Zał. Nr 3 Struktura zbiorów danych, sposób przepływu danych i zakres ich przetwarzania
- Zał. nr 4 Wykaz osób upoważnionych do przetwarzania danych osobowych
- Zał. Nr 5 Wzór upoważnienia do przetwarzania danych osobowych
- Zał. Nr 6 Klauzula poufności
- Zał. Nr 7 Ewidencja osób przetwarzających dane w przedszkolu, posiadających upoważnienia
- Zał. Nr 8 Wzór umowy powierzenia danych
- Zał. Nr 9 Wniosek o udostępnienie danych ze zbioru danych osobowych
- Zał. Nr 10 Zestawienie udostępnianych danych
- Zał. Nr 11 Wykaz podmiotów, którym powierzono przetwarzanie danych
- Zał. Nr 12 Regulamin poczty elektronicznej
- Zał. Nr 13 Instrukcja w sprawie określenia procedury postępowania z kluczami
- Zał. Nr 14. Instrukcja zarządzania Systemem Informatycznym
- Zał. Nr 15 Rejestr czynności przetwarzania (RCP)
- Zał. Nr 16. Procedura postepowania w sytuacji naruszenia ochrony danych

§ 20. Niniejszy dokument wchodzi w życie z dniem 23.05.2018r.

……
Administrator danych osobowych

Załącznik nr 1
do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Wykaz budynków i pomieszczeń

Dane osobowe przetwarzane są w siedzibie Przedszkola " Kraina Marzeń"
w Czarnej Białostockiej

Budynek	Rodzaj dokumentów	Miejsce przechowywania

Załącznik nr 2
do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Wykaz zbiorów danych
ze wskazaniem systemów służących do ich przetwarzania

Lp.	**Nazwa zbioru danych**	**Programy zastosowane do przetwarzania danych/nazwa zasobu danych**	**Lokalizacja zbioru/zasobu**	**Miejsce przetwarzania danych**

Załącznik nr 3

do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Struktura zbiorów danych, sposób przepływu danych i zakres ich przetwarzani

KARTY ZBIORÓW

Lp.	Nazwa zbioru (dokumentu) - opis	Podstawa prawna przetwarzania	Struktura zbioru	Program	Dostęp
1					

Załącznik nr 4

do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Wykaz osób upoważnionych do przetwarzania danych osobowych

Zbiór nr	**Nazwa zbioru**	**Postać zbioru**	**Nazwiska osób**
W stosunku do pracowników			
w stosunku do dzieci			

Załącznik nr 5

do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockie

(pieczęć administratora danych)

Czarna Białostocka, ...

Upoważnienie Nr / 2018 do przetwarzania danych osobowych

I.

Na podstawie art. 29 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)

z dniem.....**r.** upoważniam Panią/Pana .....

zatrudnionego/zatrudnioną w Przedszkolu „ Kraina Marzeń" w Czarnej Białostockiej do przetwarzania danych osobowych w celach związanych z wykonywaniem obowiązków na stanowisku : ..... polegającego na: zbieraniu, utrwalaniu, organizowaniu, porządkowaniu, przechowywaniu, adaptowaniu lub modyfikowaniu, pobieraniu,

przeglądaniu, wykorzystywaniu, ujawnianiu poprzez przesłanie, rozpowszechnianiu lub innego rodzaju udostępnianiu, dopasowywaniu lub łączeniu, ograniczaniu, usuwaniu lub niszczeniu

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej i elektronicznej.

II.

Upoważniam Panią/Pana*) do przetwarzania danych osobowych zawartych w następujących zbiorach: akta osobowe, dokumentacja dziecka, program EZD, FINANSE DDJ, PŁACE, KADRY, PRZELEWY, MULTICASH, IPKO

III.

1. Upoważnienie wygasa z chwilą ustania Pana/Pani*) zatrudnienia na stanowisku pracownika biurowego

2. Jednocześnie informuję, że zobowiązany(a) jest Pan(i) do zachowania powyższych informacji w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia.

…… ……

Podpis upoważnionego *(Podpis administratora)*

Załącznik nr 6
do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

KLAUZULA POUFNOŚCI

……...

……

(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz Ustawy o Ochronie Danych Osobowych.

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach
- zachowania w tajemnicy danych osobowych do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Ustawy o Ochronie Danych osobowych a od dn. 25.05.2018 Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

……

podpis oświadczającego

Załącznik nr 7
do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Ewidencja osób przetwarzających dane w przedszkolu posiadających upoważnienia

Lp.	Imię i Nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Identyfikator/login do systemu informatycznego

Załącznik nr 8
do Polityki bezpieczeństwa przetwarzania danych osobowych w ***Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej***

WZÓR UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu …… 2018 r., w……., pomiędzy:

…….
zwanym dalej **Zleceniodawcą lub Administratorem**

a

……..
zwanym dalej **Zleceniobiorcą, Podmiotem przetwarzającym lub Procesorem**

zwanymi w dalszej części Umowy, każdą z osobna „Stroną", a łącznie „Stronami".

Zważywszy, że:

- Zleceniobiorca zawarł ze Zleceniodawcą umowę, której przedmiotem jest odpłatne świadczenie na rzecz Zleceniodawcy usług z zakresu: ……..(„Umowa Główna"),
- Zleceniobiorca w ramach świadczonych usług będzie miał dostęp do danych osobowych Zleceniodawcy.

Strony niniejszym postanawiają zawrzeć Umowę powierzenia przetwarzania danych osobowych („Umowa"), o następującej treści:

§ 1
Oświadczenia Stron

1. Procesor oświadcza, że dysponuje środkami umożliwiającymi prawidłowe przetwarzanie danych osobowych powierzonych przez Administratora, w zakresie i celu określonym Umową.
2. Procesor oświadcza również, że osobom przez niego zatrudnionym lub z nim współpracującym, przy przetwarzaniu powierzonych danych osobowych, nadane zostają upoważnienia do przetwarzania danych osobowych, oraz że osoby te zostają zapoznane z przepisami o ochronie danych osobowych i z odpowiedzialnością za ich nieprzestrzeganie, oraz zobowiązują się do ich przestrzegania i bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.
3. Procesor oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne spełniają wymogi aktualnie obowiązujących przepisów prawa.
4. Podmiot przetwarzający oświadcza, że dysponuje zasobami, doświadczeniem, wiedzą fachową i wykwalifikowanym personelem, które umożliwiają mu prawidłowe wykonanie Umowy oraz wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi 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).

5. Podmiot przetwarzający oświadcza, że podjął skuteczne środki techniczne i organizacyjne zabezpieczające dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz uszkodzeniem, zniszczeniem, utratą lub nieuzasadnioną modyfikacją.

§ 2

Cel, zakres, miejsce, rodzaj danych, kategorii osób, charakter przetwarzania powierzonych danych osobowych

1. Administrator powierza Procesorowi przetwarzanie danych osobowych w zakresie i celu niezbędnym do realizacji przedmiotu Umowy Głównej, tj.:
   a) Powierzenie przetwarzania danych osobowych obejmuje następujące kategorie osób, których dane dotyczą: ……
   b) Rodzaj powierzonych do przetwarzania danych osobowych: dane zwykłe i/lub dane należące do szczególnej kategorii danych osobowych.
2. Na wniosek osoby, której dane dotyczą, Procesor wskaże miejsca, w których przetwarza powierzone dane.
3. Podmiot przetwarzający będzie przetwarzał dane osobowe w formie papierowej i/lub przy wykorzystaniu systemów informatycznych. Przez przetwarzanie danych osobowych rozumie się wszelkie operacje wykonywanych na danych osobowych, 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.

§ 3

Zasady przetwarzania danych osobowych

1. Podmiot przetwarzający zobowiązuje się:
   a) Wykonywać zobowiązania wynikające z Umowy z najwyższą starannością zawodową w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów Administratora w zakresie przetwarzania powierzonych danych osobowych.
   b) Do przetwarzania powierzonych danych osobowych wyłącznie na podstawie Umowy, zgodnie z Umową oraz obowiązującymi przepisami dotyczącymi ochrony danych osobowych oraz w celach związanych z realizacją Umowy Głównej i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów.
   c) Przetwarzać powierzone mu dane osobowe wyłącznie na terytorium Europejskiego Obszaru Gospodarczego.
   d) Przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Administratora.
   e) Niezwłocznego informowania Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych.
   f) Udzielać dostępu do powierzonych danych osobowych wyłącznie osobom, które ze względu za zakres wykonywanych zadań otrzymały od Procesora upoważnienie do ich przetwarzania oraz wyłącznie w celu wykonywania obowiązków wynikających z Umowy.
   g) Do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, w tym także po rozwiązaniu Umowy oraz zobowiązuje się zapewnić, aby jego pracownicy oraz inne osoby upoważnione do przetwarzania powierzonych danych osobowych, zobowiązały się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, w tym także po rozwiązaniu Umowy.
   h) Zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
   i) Wspierać Administratora w realizacji obowiązku odpowiadania na żądania osób, których dane dotyczą, w wykonywaniu ich praw określonych w rozdziale III RODO, w szczególności niezwłocznie na żądanie Administratora, nie później jednak niż w terminie 5 dni od daty zgłoszenia takiego żądania Procesor udzieli informacji dotyczących powierzonych mu do przetwarzania danych osobowych, w tym zastosowanych technicznych i organizacyjnych środków zabezpieczenia danych osobowych.
   j) Pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO. W szczególności niezwłocznie, nie później jednak niż w ciągu 24 godzin od momentu stwierdzenia naruszenia, informować Administratora o każdym naruszeniu ochrony danych osobowych (jego skali, charakterze, podjętych działaniach naprawczych, tożsamości podmiotów danych dotkniętych naruszeniem oraz ryzyku, jakie naruszenie może powodować dla podmiotów danych), a także przekazać Administratorowi informacje o stosowanych środkach zabezpieczenia danych osobowych oraz zawiadomić o naruszeniu osoby, których dane osobowe dotyczą, **o ile**

zażąda tego Administrator. Do czasu uzyskania instrukcji od Administratora Podmiot przetwarzający podejmuje wszelkie, rozsądne działania mające na celu ograniczenie i naprawienie negatywnych skutków zdarzenia;

k) Do prowadzenia rejestru wszystkich kategorii czynności przetwarzania (art. 30 ust. 2 – 5 RODO).

l) Udostępniać Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w Umowie oraz umożliwiać Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczyniać się do nich.

m) Niezwłocznie, jednak nie później niż w ciągu 2 (dwóch) dni roboczych informować (o ile nie doprowadzi to do naruszenia przepisów obowiązującego prawa) Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych przez Procesora, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania danych osobowych, skierowanej do Procesora, o wszelkich kontrolach i inspekcjach dotyczących przetwarzania danych osobowych przez Procesora.

n) Niezwłocznie aktualizować, poprawiać, zmieniać, anonimizować, ograniczać przetwarzanie lub usuwać wskazane dane osobowe zgodnie z wytycznymi Administratora (jeżeli działanie te mogłoby powodować brak możliwości dalszego realizowania czynności przetwarzania, Procesor poinformuje Administratora przed jego podjęciem, a następnie zastosuje się do polecenia Administratora).

§ 4

Podpowierzenie

1. Administrator wyraża zgodę na dalsze powierzenie przez Procesora powierzonych do przetwarzania danych osobowych innym podmiotom przetwarzającym, w zakresie oraz w celu zgodnym z Umową, zwanym dalej „dalszym podmiotem przetwarzającym". Procesor jest zobowiązany do informowania Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia dalszych podmiotów przetwarzających drogą elektroniczną na adres e-mail Administratora wskazany w Umowie (w formie dokumentowej). Podmiot przetwarzający może powierzyć dane osobowe dalszemu podmiotowi przetwarzającemu, o ile Administrator, w ciągu 7 dni roboczych od dnia wysłania wiadomości nie zgłosi sprzeciwu. Administrator zgłasza sprzeciw w formie dokumentowej na adres e-mail Procesora, wskazany w Umowie.
2. Na dzień podpisania Umowy – listę dalszych podmiotów przetwarzających, zawiera załącznik nr 1 do Umowy. Administrator wyraża zgodę na powierzenie tym podmiotom danych osobowych, o których mowa w Umowie.
3. W przypadku podpowierzenia, Procesor zapewnia, że będzie korzystał wyłącznie z usług takich dalszych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz przepisów obowiązującego prawa z zakresu ochrony danych osobowych, a także chroniło prawa osób, których dane dotyczą.
4. Procesor zapewni, że w umowie z dalszym podmiotem przetwarzającym, zostaną nałożone na ten podmiot obowiązki odpowiadające obowiązkom Procesora określonym w Umowie.
5. Procesor jest w pełni odpowiedzialny przed Administratorem za spełnienie obowiązków wynikających z umowy powierzenia zawartej pomiędzy Procesorem, a dalszym podmiotem przetwarzającym. Jeżeli Podmiot przetwarzający nie wypełni spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków dalszego podmiotu przetwarzającego spoczywa na Procesorze.

§ 5

Czas trwania Umowy oraz odpowiedzialność Stron

1. Umowa obowiązuje przez czas obowiązywania Umowy Głównej.
2. Umowa wchodzi w życie z dniem podpisania.
3. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że szczególne przepisy prawa nakazują przechowywanie danych osobowych.
4. Zleceniobiorca ponosi odpowiedzialność za przestrzeganie przepisów prawa w zakresie przetwarzania i ochrony danych osobowych według RODO.
5. Powyższe nie wyłącza odpowiedzialności Zleceniobiorcy za przetwarzanie powierzonych danych niezgodnie z Umową.
6. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem, w szczególności jeśli nie dopełnił obowiązków, które nakłada na niego Umowa lub przepisy prawa, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom.

§ 6

Uprawnienia kontrolne Administratora

1. Administrator lub upoważniony przez niego audytor zewnętrzny ma prawo do przeprowadzenia kontroli przestrzegania przez Podmiot przetwarzający zasad przetwarzania danych osobowych, o których mowa w Umowie oraz w

obowiązujących przepisach prawa, w szczególności poprzez żądanie udzielenia informacji dotyczących przetwarzania danych przez Podmiot przetwarzający, stosowanych środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z prawem lub dokonywanie kontroli w miejscach, w których są przetwarzane powierzone dane osobowe, po wcześniejszym uzgodnieniu terminu przez Strony, na 10 dni przed planowaną kontrolą. Podmiot przetwarzający dokona niezbędnych czynności w celu umożliwienia wykonania tego uprawnienia przez Administratora.

2. Podmiot przetwarzający jest zobowiązany do stosowania się do zaleceń Administratora dotyczących zasad przetwarzania powierzonych danych osobowych oraz dotyczących poprawy zabezpieczenia danych osobowych, sporządzonych w wyniku kontroli przeprowadzonych przez Administratora lub upoważnionego przez niego audytora.

§ 7
Postanowienia końcowe

1. Strony wskazują następujące adresy e-mail do doręczeń:
   a) Procesor …….
   b) Administrator ……..
2. Wszelkie zmiany, uzupełnienia, rozwiązanie lub wypowiedzenie Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
3. W zakresie nieuregulowanym Umową zastosowanie mają przepisy w szczególności Kodeksu cywilnego.
4. W przypadku, gdy Umowa odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
6. Załączniki stanowią integralną część Umowy.
7. Postanowienia Umowy zastępują dotychczasowe postanowienia dotyczące danych osobowych.

…….. ……
Zleceniodawca Zleceniobiorca

Załącznik nr 1 do Umowy – Lista dalszych podmiotów przetwarzających

1. …….
2. …….

Załącznik nr 9
do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Wniosek o udostępnienie danych
ze zbioru danych osobowych

1. Wniosek do: . . . . . .

2. Wnioskodawca: . . . . . .
(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy ew. NIP oraz REGON)

3. Podstawa prawna upoważniająca do pozyskania danych: . . . . . .
4. Wskazanie przeznaczenia dla udostępnionych danych osobowych: . . . . . .
5. Oznaczenia lub nazwa zbioru, z którego mają być udostępnione dane osobowe: . . . . . .
6. Zakres żądanych informacji ze zbioru: . . . . . .
7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych: . . . . . .

.

. . . . . .
(data i podpis wnioskodawcy)

Załącznik nr 10
do Polityki bezpieczeństwa przetwarzania danych osobowych w ***Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej***

Rejestr udostępnianych danych

Lp.	Rodzaj udostępnionych danych osobowych	Data udostępnienia danych	Imię i nazwisko osoby, która udostępniła dane	Imię i nazwisko osoby, która otrzymała dane / dane podmiotu	Cel przekazania

Załącznik nr 11
do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Wykaz podmiotów, którym powierzono przetwarzanie danych

Lp.	Nazwa podmiotu	Data zawarcia umowy powierzenia

Załącznik nr 12
do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

REGULAMIN POCZTY ELEKTRONICZNEJ W PRZEDSZKOLU „KRAINA MARZEŃ" W CZARNEJ BIAŁOSTOCKIEJ

Rozdział 1
Postanowienia ogólne

§1. Przedszkole „Kraina Marzeń" w Czarnej Białostockiej określa w niniejszym regulaminie zasady udostępniania kont pocztowych (zwanych dalej Kontami Pocztowymi) w ramach systemu poczty elektronicznej Przedszkola.
§2. 1 System poczty elektronicznej Przedszkola dostępny jest na zasadach określonych w niniejszym Regulaminie.
2. E-maile wysyłane ze służbowej skrzynki pocztowej stanowią własność pracodawcy.
3. Każdy użytkownik zobowiązany jest do zapoznania się z poniższym Regulaminem.
4. Konto pocztowe w domenie ***home.pl*** jest przeznaczone tylko i wyłącznie do wykorzystania w zakresie działalności zawodowej.

§ 3. Nadzór i opiekę techniczną nad systemem poczty elektronicznej sprawuje informatyk.
§ 4. 1. System poczty elektronicznej Przedszkola posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem przez osoby trzecie.

2. Dostęp do Konta Pocztowego jest chroniony hasłem. Hasło stanowi zabezpieczenie dostępu do systemu oraz treści wiadomości przechowywanych na Koncie Pocztowym. Z uwagi na bezpieczeństwo systemu pocztowego oraz danych Użytkownika hasło musi być tajne, to znaczy znane wyłącznie Użytkownikowi. W przypadku odtajnienia hasła należy niezwłocznie zmienić je na nowe.
3. Hasło nie może być zbyt proste lub oczywiste do odgadnięcia przez osoby trzecie. **Może** spełniać warunki:
1) zawierać co najmniej 8 znaków,
2) zawierać co najmniej 1 dużą literę,
3) zawierać co najmniej 1 małą literę,
4) zawierać co najmniej 1 cyfrę lub znak specjalny, np. % itp.

Rozdział 2
Udostępnienie i Użytkowanie Konta Pocztowego

§ 5. Rozpoczynając korzystanie z konta pocztowego Użytkownik zgadza się na gromadzenie, przetwarzanie oraz wykorzystywanie podanych informacji o sobie przez Przedszkole wyłącznie w celach technicznych, statystycznych zgodnie ustawą o ochronie danych osobowych.
§ 6. Przedszkole zobowiązuje się, iż nie będzie udostępniać zebranych danych osobom trzecim. Wyjątki od tej zasady mogą być spowodowane wyłącznie nakazem organów państwowych.
§ 7. Dostęp do Konta Pocztowego możliwy jest za pomocą przeglądarki internetowej poprzez stronę internetową: ***www.home.pl***
§ 8. Użytkownik:

1) ma obowiązek zapoznania się z treścią niniejszego Regulaminu;
2) ma obowiązek regularnego sprawdzania służbowej poczty elektronicznej- codziennie;
3) bezzwłocznego odpowiadania na e-maile;
4) ma prawo otrzymywać korespondencję dotyczącą wydarzeń związanych z Przedszkolem;
5) jest zobowiązany do korzystania z adresu e-mail zgodnie z obowiązującymi przepisami, normami społecznymi i obyczajowymi;
6) nie może wykorzystywać służbowej skrzynki w celach prywatnych;
7) ponosi odpowiedzialność za treść i zawartość listów przesyłanych za pośrednictwem jego adresu e-mail.
8) ma prawo korzystać ze Konta Pocztowego w pełnym zakresie jego funkcjonalności pod warunkiem, że będzie to zgodne z obowiązującym prawem, normami społecznymi i obyczajowymi.
9) przed rozpoczęciem użytkowania skrzynki pocztowej składa oświadczenie wg wzoru.

§ 9. Przedszkole zastrzega sobie prawo do:

1) awaryjnego wyłączenia systemu bez uprzedniego powiadomienia Użytkowników;
2) zamykania kont osób, które przestają być pracownikami Przedszkola;
3) zablokowania konta w przypadkach wykorzystania konta do prywatnej działalności komercyjnej lub naruszających ogólnie przyjęte zasady współistnienia użytkowników sieci Internet.

§ 10. Przedszkole nie ponosi odpowiedzialności za:

1) skutki wejścia przez osoby trzecie w posiadanie hasła umożliwiającego korzystanie z konta;
2) utratę danych spowodowaną awarią sprzętu;
3) przerwy w funkcjonowaniu systemu pocztowego zaistniałe z przyczyn technicznych.

Rozdział 3
Postanowienia końcowe

§ 11. 1. Przedszkole zastrzega sobie prawo do zmiany postanowień niniejszego Regulaminu.
2. Regulamin korzystania z poczty elektronicznej obowiązuje pracowników administracji od 16.07.2018r. zaś nauczycieli od 27.08.2018r.

Wzór oświadczenia

Potwierdzam zapoznanie się z Regulaminem Poczty Elektronicznej w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej oraz zasadami i zaleceniami odnośnie bezpieczeństwa i korzystania ze służbowego konta pocztowego.

Oświadczam, że dnia …… otrzymałam/ - em login i hasło do własnego służbowego konta pocztowego

adres e-mail

Imię i nazwisko ……
Stanowisko ……...

. . . . . *.data, podpis pracownika*

Załącznik nr 13
do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Instrukcja w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia w budynku Przedszkola „Kraina Marzeń" w Czarnej Białostockiej

Rozdział 1

Obowiązki pracowników w zakresie postępowania z kluczami oraz zabezpieczenia pomieszczeń biurowych

§1. 1.Ustala się następujące zasady postępowania z kluczami oraz zabezpieczenia pomieszczeń biurowych:

6) klucze od poszczególnych pomieszczeń służbowych są w ciągłym posiadaniu pracowników administracji, którzy własnoręcznym podpisem złożonym na liście użytkownik/posiadacz kluczy potwierdzili ich odbiór, ponosząc pełną odpowiedzialność za ich należyte zabezpieczenie. Wzór listy stanowi załącznik Nr 1 do niniejszych procedur.

7) klucza nie wolno przekazywać/udostępniać innej osobie pod żadnym pozorem, drzwi otwiera i zamyka pracownik, który pokwitował odbiór klucza.

8) Pomieszczenie służbowe, w którym chwilowo nie przebywa żaden pracownik powinno być zamknięte na klucz.

9) Klucze od biurek stanowiskowych, szaf biurowych, kasetek metalowych są w ciągłym posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.

10) Po otwarciu pomieszczeń biurowych, jeszcze przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, a także składowanej w tych pomieszczeniach dokumentacji innego wyposażenia.

11) W przypadku stwierdzenia zmian lub naruszenia stanu zabezpieczeń, pracownik, który to stwierdził, natychmiast powiadamia o tym dyrektora Przedszkola.

12) Po zakończeniu dnia pracy, pracownicy administracji Przedszkola zobowiązani są do uporządkowania swoich stanowisk pracy, wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych, w szczególności: zabezpieczenia komputerów i wszelkich nośników danych, wyłączenia wszystkich urządzeń elektrycznych (nie wymagających stałego zasilania), zamknięcia wszystkich okien i drzwi.

13) Pracownik przedszkola chcąc kontynuować prace poza normalnymi godzinami pracy, może uzyskać zgodę dyrektora- w ściśle uzasadnionych przypadkach.

14) Konserwator i pracownik gospodarczy dysponują kompletami kluczy do drzwi wejściowych Przedszkola i ponoszą pełną odpowiedzialność za ich zabezpieczenia przed utratą. Bezwzględnie nie mogą ich udostępniać pozostałym pracownikom. Pracownik gospodarczy ponosi pełną odpowiedzialność za zamknięcie drzwi zewnętrznych wejściowych po skończonej pracy.

15) Zgubienie klucza, przekazanie innej osobie lub utrata w jakikolwiek inny sposób może skutkować dla pracownika konsekwencjami służbowymi lub dyscyplinarnymi.

§ 2.1. Duplikaty kluczy do pomieszczeń, w których przechowywane są dokumenty zawierające dane osobowe będące kluczami zapasowymi do pomieszczeń Przedszkola są przechowywane w szafce metalowej, przyjmowane za pokwitowaniem i podlegają zabezpieczeniu przez wyznaczonego pracownika w sposób uniemożliwiający pobranie ich przez osobę nieuprawnioną.
2. Wydanie kluczy zapasowych, o których mowa w ust.1, uprawnionym do ich pobrania pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz w przypadkach awaryjnych za zgodą bezpośredniego przełożonego – za pokwitowaniem w odpowiednim rejestrze wraz z uzasadnieniem konieczności wydania kluczy.
3. Klucze zapasowe, po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu za poświadczeniem zwrotu w rejestrze.
4. Wzór rejestru, o którym mowa w ust.2, - „Ewidencji użytkowników/posiadaczy kluczy zapasowych" stanowi załącznik Nr 2 do niniejszej instrukcji.

§ 3. 1 Z uwagi na publiczny charakter funkcjonowania Przedszkola, w godzinach otwarcia nie stosuje się sformalizowanego systemu uprawnień do wchodzenia i przebywania na terenie budynku. Stan ten poszerza zakres obowiązków wszystkich pracowników Przedszkola, którzy są zobowiązani do:
1) reagowania na wejście i przebywanie osób będących pod wpływem alkoholu lub środków odurzających,
2) reagowania na próby wnoszenia do budynku przedmiotów lub materiałów niebezpiecznych lub substancji budzących podejrzenie,
3) reagowania na próby niszczenia, wynoszenia lub wywożenia mienia z budynku Przedszkola
4) niezwłocznego reagowania na zaobserwowane próby stwarzania zagrożenia dla życia lub zdrowia osób a także utraty lub zniszczenia mienia.

§ 4. 1. Pomieszczeniami podlegającymi szczególnej ochronie są: składnica akt, pomieszczenia administracji, pomieszczenie z kluczami.
2. Sprzątanie pomieszczeń wymienionych w ust. 1 odbywa się w godzinach pracy Przedszkola.

§ 5. Zabrania się:
4) dorabiania kluczy do pomieszczeń i budynku Przedszkola bez zgody Dyrektora udzielonej ustnie i / lub na piśmie,

5) udostępniania kluczy oraz kodów sterujących systemem alarmowym osobom nieupoważnionym,

6) pozostawiania otwartych pomieszczeń lub kluczy bez dozoru.

§ 6. 1. Pełny dostęp do budynku Przedszkola posiadają osoby dysponujące odpowiednimi kompletami kluczy oraz kodami umożliwiającymi otwarcie drzwi zewnętrznych i wyłączenie funkcji czuwania systemu alarmowego: dyrektor, konserwator, pracownik gospodarczy.
2. Osoby uprawnione, z osób wymienionych w ust. 1, potwierdzą w złożonych upoważnieniach, odbiór kompletów kluczy do drzwi zewnętrznych wraz z kodami dostępu (wzór upoważnienia stanowi załącznik Nr 3 do niniejszych procedur).
3. Prawo do otwierania wszystkich pomieszczeń służbowych wewnątrz budynku Przedszkola dla skontrolowania przestrzegania przez zobowiązane osoby postanowień niniejszej procedury posiada Dyrektor.

§ 7.1. Otwarcia pomieszczeń przedszkola po porze nocnej dokonuje wyznaczony pracownik (konserwator) na podstawie zakresu obowiązków pomiędzy godzina 5.30 – 6.00.
2. Zamkniecie budynku Przedszkola po zakończeniu dnia pracy i załączeniu systemu alarmowego w obiekcie dokonuje pracownik gospodarczy, a w razie jego nieobecności sprzątaczka.

Rozdział II

Obsługa systemu alarmowego

§ 8.1. Budynek Przedszkola wyposażony jest w urządzenie alarmowe i osoba dokonująca otwarcia budynku, dokonuje równocześnie wyłączenia czuwania systemu alarmowego w całym obiekcie.
2. Załączenia czuwania systemu alarmowego dokonuje upoważniony pracownik wykonujący prace na stanowisku pracownika gospodarczego lub w razie jego nieobecności sprzątaczka.
3. Osoba dokonująca otwarcia budynku Przedszkola w sytuacjach nadzwyczajnych, w dni wolne od pracy lub w godzinach nocnych (tj. w godz. od 21.00 do 5.30) zobowiązana jest do telefonicznego powiadomienia o powyższym Dyrektora Przedszkola.

Rozdział III

Postanowienia końcowe

§ 9. Odpowiedzialnymi za realizację zasad, o których w niniejszej instrukcji są wszyscy pracownicy zatrudnieni w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej.

Załącznik Nr 1 do instrukcji w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń w budynku Przedszkola „Kraina Marzen" w Czarnej Białostockiej.

Lista użytkowników/posiadaczy kluczy do pomieszczeń w budynku Przedszkola „Kraina Marzeń" w Czarnej Białostockiej

Lp.	Imię i Nazwisko	Stanowisko	Nr pomieszczenia/drzwi	Data i podpis
1.	Danuta Kowalewska	dyrektor	1.20 1.22 skrzynka do alarmu, drzwi wejściowe (zew.i wew.) od ulicy Wiosennej i Jastrzębiej	
2.	Agnieszka Radkowska	wicedyrektor	1.20, 1.22	
3.	Krystyna Poskrobko	Główna księgowa	1.21	
4.	Beata Pietraniuk	Intendent- kasjer	1. 1	
6.	Mikołaj Czarniecki	Pracownik gospodarczy	0.13 drzwi wejściowe (zew.i wew.) od ulicy Wiosennej, skrzynka do alarmu, brama i bramka od ul. Wiosennej bramka od ul. Jastrzębiej bramki od ul. Torowej	
7.	Grzegorz Biruk	konserwator	0.13 drzwi wejściowe (zew.i wew.) od ulicy Wiosennej, skrzynka do alarmu, brama i bramka od ul. Wiosennej bramka od ul. Jastrzębiej bramki od ul. Torowej	
8.	Beata Matejczyk	sekretarka	1.1	

Załącznik Nr 2 o instrukcji w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń w budynku Przedszkola „Kraina Marzen" w Czarnej Białostockiej.

Ewidencja użytkowników/posiadaczy kluczy zapasowych do pomieszczeń w budynku Przedszkola „Kaina Marzeń" w Czarnej Białostockiej.

L.p.	Imię i Nazwisko	Stanowisko	Nr pomieszczenia	Data pobrania kluczy i podpis	Data zwrotu kluczy i podpis

Załącznik Nr 3 o instrukcji w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń w budynku Przedszkola „Kraina Marzen" w Czarnej Białostockiej.

Upoważnienie da zarządzania kluczami oraz kodem cyfrowym do systemu alarmowego do budynku Przedszkola „Kraina Marzeń" w Czarnej Białostockiej

Na podstawie instrukcji w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń budynku Przedszkola „Kraina Marzeń" w Czarnej Białostockiej powierzam Panu **……** zatrudnionemu na stanowisku pracownika gospodarczego komplet kluczy do budynku Przedszkola „Kraina Marzeń" w Czarnej Białostockiej.

W skład kompletu wchodzą następujące klucze:……

Ponadto przydzielam Panu kod cyfrowy do systemu alarmowego, który należy zachować w ścisłej tajemnicy i wykorzystywać zgodnie z postanowieniami w/w instrukcji.

…… ……
(data i podpis pracodawcy) (podpis pracownika)

Oświadczenie pracownika

Oświadczam, że przyjmuję pełna odpowiedzialność za powierzone klucze oraz kod cyfrowy do sytemu alarmowego i zobowiązuje się do ich wykorzystania jedynie w celach realizacji powierzonych mi zadań zgodnie z niniejszym upoważnieniem.

…….....
(data i podpis pracownika)

Załącznik nr 14

do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Instrukcja Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń"" w Czarnej Białostockiej

I. CELE WPROWADZENIA I ZAKRES ZASTOSOWANIA INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM.

1. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Przedszkolu "Kraina marzeń" w Czarnej Białostockiej , zwana dalej instrukcją, została wprowadzona na podstawie ustawy z 10 maja 2018r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000) oraz 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 95/49/WE, w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Instrukcja jest dokumentem powiązanym z „Polityką bezpieczeństwa" w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej i wraz z nim składa się na dokumentację wymaganą przez art. 36. ust. 2. ustawy o ochronie danych osobowych.

3. Niniejsza instrukcja znajduje zastosowanie do systemów informatycznych, stosowanych w przedszkolu, w których są przetwarzane dane osobowe.

4. Instrukcja podlega monitorowaniu przez administratora danych osobowych lub upoważnioną przez niego osobę, w ramach sprawowania kontroli zarządczej.

5. Dokument instrukcji przechowywany jest w wersji papierowej i elektronicznej.

II. DEFINICJE.

1. Definicje:

Ilekroć w instrukcji jest mowa o:

1) administratorze danych osobowych – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych. W Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej funkcję administratora danych pełni dyrektor przedszkola;

2) administratorze bezpieczeństwa informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji (ABI) a od 25 maja 2018 r. Inspektora Ochrony Danych (IODO);

3) administratorze systemu informatycznego – rozumie się przez to osobę nadzorującą pracę systemu informatycznego oraz wykonującą w nim czynności wymagających specjalnych uprawnień lub wiedzy;

4) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

5) zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów;

6) przetwarzanie danych – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywania, udostępnianie, zmienianie, usuwanie;

7) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

8) identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

9) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

10) osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to pracownika przedszkola, która upoważniona została do przetwarzania danych osobowych przez dyrektora przedszkola na piśmie;

11) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;

12) raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

13) rozporządzeniu MSWiA – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych (Dz.U. z 2004 r., nr 100, poz. 1024.);

14) serwisancie – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;

15) sieci publicznej – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;

16) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

17) przedszkole – rozumie się przez to Przedszkole „ Kraina Marzeń w Czarnej Białostockiej;

18) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

19) ustawie – rozumie się przez to ustawę z 10 maja 2018r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

20) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

21) użytkowniku – rozumie się przez to pracownika przedszkola upoważnionego do przetwarzania danych osobowych, zgodnie z zakresem obowiązków, któremu nadano identyfikator i przyznano hasło.

III. NADAWANIE I REJESTROWANIE (WYREJESTROWANIE) UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM.

1. Nadawanie i rejestrowanie uprawnień.

1) Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona przez Administratora Bezpieczeństwa Informacji do przetwarzania danych osobowych, po wydaniu zaświadczenia Administratora Danych Osobowych zarejestrowana jako użytkownik w tym systemie przez dyrektora przedszkola lub uprawnioną przez niego osobę.

2) Rejestracja użytkownika, o którym jest mowa w pkt. 1., polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

2. Wyrejestrowanie uprawnień.

1) Wyrejestrowanie użytkownika systemu informatycznego dokonuje dyrektor przedszkola lub upoważniona przez niego osoba.

2) Wyrejestrowanie, o którym jest mowa w pkt. 1., może mieć charakter czasowy lub trwały.

3) Wyrejestrowanie następuje przez:

a) zablokowanie konta użytkownika do czasu ustania przyczyny, uzasadniającej blokadę (wyrejestrowanie czasowe),

b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4) Czasowe wyrejestrowanie użytkownika z systemu musi nastąpić w razie:

a) nieobecności użytkownika w pracy, trwającej dłużej niż 30 dni kalendarzowych,

b) zawieszenia w pełnieniu obowiązków służbowych.

5) Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:

a) wypowiedzenie umowy o pracę,

b) wszczęcie postępowania dyscyplinarnego.

6) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

IV. METODY I ŚRODKI UWIERZYTELNIENIA.

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie

2. Hasło użytkownika powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

3. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

4. Zmiana haseł w systemie następuje nie rzadziej niż co 30 dni.

5. Hasło nie może być zapisywane i przechowywane

V. PROCEDURY ZWIĄZANE Z GROMADZENIEM, PRZECHOWYWANIEM, PRZETWARZANIEM, USUWANIEM DANYCH OSOBOWYCH.

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informacyjnym oraz wskazanie osoby odpowiedzialnej za te czynności.

1) Przetwarzać dane osobowe w systemie informatycznym może wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych (wzór tego upoważnienia stanowi *załącznik nr 5* do Polityki ochrony danych osobowych

2.) Identyfikator i hasło do systemu informatycznego, przetwarzającego dane osobowe, są przydzielone użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada administrator systemu informatycznego. Wyrejestrowanie użytkownika z systemu informatycznego następuje na wniosek administratora danych osobowych.

3) Wyznaczona osoba jest zobowiązany do prowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła, oraz uzyskaniu zaświadczenia do przetwarzania danych osobowych, zaświadczenie jest także niezbędne do przetwarzania danych osobowych w systemie tradycyjnym.

2) Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiada za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje.

3) Identyfikator i hasło użytkownika powinny odpowiadać wymaganiom, określonym w rozdziale IV.

4) Nazwy i hasła użytkowników, posiadających uprawnienia do informatycznego przetwarzania danych osobowych, powinny być przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do nich mają wyłącznie osoby uprawnione. Nazwy i hasła użytkowników powinny być przechowywane w opieczętowanej i opatrzonej pieczęcią przedszkola i podpisem administratora systemu informatycznego w kopercie.

5) W przypadku konieczności użycia nazw i haseł tych użytkowników konieczny jest wpis, ilustrujący zaistniałą sytuację w „Dzienniku haseł", który jest przechowywany w szafie zamykanej na klucze, wraz z kopertą, w której znajdują się hasła. Wpis powinien zawierać następujące informacje:

a) imię i nazwisko oraz stanowisko osoby upoważnionej, udostępniającej dostęp do szafy, w której znajdują się hasła,

b) imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,

c) krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

6) O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony administrator bezpieczeństwa informacji oraz administrator danych.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1) Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy, mogące świadczyć o naruszeniu ochrony danych osobowych.

2) Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

3) W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 10 minut - automatycznie włączony jest wygaszasz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu.

4) Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólne konto użytkownika.

5) W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut - użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje, oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki informacji, zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

6) Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

4. Procedury tworzenia i sposobu przechowywania kopii zapasowych

1)Dane osobowe, zabezpiecza się poprzez wykonywanie

2) Kopie zapasowe informacji przechowywanych w systemie informatycznym, przetwarzającym dane osobowe, tworzone są w następujący sposób:

a) Kopie zapasowe mogą byc sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze

b) Kopia zapasowa danych osobowych przetwarzanych przez aplikację (pełna kopia) wykonywana jest raz w tygodniu na dysku komputera wybranego przez administratora systemu informatycznego,

3) Pliki edytorów tekstu lub arkuszy kalkulacyjnych traktowane są jak kopie zbiorów z których pochodzą przetwarzane w nich dane i nie są objęte procedurami wykonywania kopii zapasowych

4) Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych danych.

5. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego, przetwarzającego dane osobowe, muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

2) Prace serwisowe na terenie przedszkola, prowadzone w tym zakresie, mogą być wykonywane wyłącznie przez jego pracowników lub przez upoważnionych przedstawicieli wykonawców zewnętrznych, znajdujących się w towarzystwie pracowników przedszkola.

3) Przed rozpoczęciem prac serwisowych przez osoby spoza przedszkola konieczne jest potwierdzenie tożsamości serwisantów.

4) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

• likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

• przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

• naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

VI. STOSOWANE ŚRODKI BEZPIECZEŃSTWA

1. W przedszkolu stosuje się następujące środki bezpieczeństwa:

1) Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2) Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

3) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.

5) W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni - Hasło składa się co najmniej z 8 znaków.

6) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów, służących do przetwarzania danych osobowych.

7) Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności.

8) Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

9) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

10) W przypadku, gdy do uwierzytelnienia użytkowników używa się haseł, hasło to składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.

11) Urządzenia i nośniki, zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

12) Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

VII. POSTANOWIENIA KOŃCOWE.

1. Osobą odpowiedzialną za przegląd przestrzegania instrukcji, przegląd jej aktualności oraz aktualizację, a także nadawanie praw dostępu do systemu informatycznego jest administrator systemu informatycznego lub inna osoba upoważniona przez administratora danych.

2. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.

4. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52. kodeksu pracy.

5. Niniejsza instrukcja wchodzi w życie z dniem …..23.05.2018r. .....

Załącznik nr 15

do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń” w Czarnej Białostockiej

REJESTR CZYNNOŚCI PRZETWARZANIA (RCP)

CEL PRZETWA-RZANIA	KATEGO-RIA OSÓB,	KATEGORIE DANYCH	PLANOWA-NY TERMIN USUNIĘCIA KATEGORII DANYCH	NAZWA WSPÓŁ-ADMINI-STRAT-ORA I DANE KONTA-KTOWE	NAZWA PODMIOTU PRZETWARZA JĄCEGO DANE KONTAKTOW E	KATEGORIE ODBIORCÓ W	OGÓLNY OPIS TECHNICZNY I ORGANIZACYJ NYCH ŚRODKÓW BEZPIECZEŃST WA	TRANSFER DO KRAJU TRZECIEGO LUB ORGANIZACJI MIĘDZYNARODO WEJ

Załącznik nr 16

do Polityki bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych w Przedszkolu „Kraina Marzeń" w Czarnej Białostockiej

Istota naruszenia danych osobowych

§ 1. 1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) nieautoryzowany dostęp do danych,
2) nieautoryzowane modyfikacje lub zniszczenie danych,
3) udostępnienie danych nieautoryzowanym podmiotom,
4) nielegalne ujawnienie danych,
5) pozyskiwanie danych z nielegalnych źródeł.

Postępowanie w przypadku naruszenia danych osobowych

§ 2.1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Inspektorowi ochrony danych.

2. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych:
    1) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
    2) dokumentacja jest niszczona bez użycia niszczarki;
    3) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
    4) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), zdjęciach, płytach CD w formie niezabezpieczonej itp.
    5) nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,
    6) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
    7) wynoszenie danych osobowych (dokumentów zawierających dane osobowe np. listy płac, zaświadczenia, dzienniki zajęć, karty obserwacji, diagnozy, opinie i orzeczenia wydane przez poradnie itp.) wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;

8) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
9) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
10) telefoniczne próby wyłudzenia danych osobowych; udzielenie informacji telefonicznych nieuprawnionej osobie do uzyskania tych informacji;
11) kradzież komputerów lub twardych dysków z danymi osobowymi;
12) utrata kontroli nad kopią danych osobowych;
13) praca przy przetwarzaniu danych osobowych osoby nieprzeszkolonej lub/i nieposiadającej upoważnienia do przetwarzania danych osobowych wydanego przez Administratora;
14) maile zachęcające do ujawnienia identyfikatora i/lub hasła;
15) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
16) hasła do systemów przechowywane są w pobliżu komputera.

§ 3. Każdy pracownik Przedszkola, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .

§ 4. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora danych.

§ 5. Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora ochrony danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6. Inspektor ochrony danych podejmuje następujące kroki:
1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
2) odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
3) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7. Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych

§8. Inspektor ochrony danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) - Załącznik nr 1 - rejestr incydentów i działań korygujących i zapobiegawczych.

Naruszenie danych osobowych - odpowiedzialność

§ 9. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

§ 10.1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności

Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych								
Zadanie / problem / incydent	**Źródło zgłoszenia**	**Data rozpoczęcia**	**Data zakończenia**	**Czy koniec?**	**Odpowiedzialny za realizację**	**Przyczyna niezgodności**	**Działanie korygujące / zapobiegawcze**	**Ocena skuteczności**

osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

§ 11.1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1 opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 lit. b), c) i d).

3.Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych; b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

mgr DANUTA KOWALEWSKA
Dyrektor
Przedszkola „KRAINA MARZEŃ"
w Czarnej Białostockiej