Polityka Bezpieczeństwa Danych Osobowych

w

Szkole Podstawowej nr 3 Przymierza Rodzin **im. bł. ks. Jerzego Popiełuszki**

Data przyjęcia dokumentu:

Ważny od: 01.04.2019r.

W imieniu Administratora Danych Osobowych

Dyrektor
Mirosława Piasecka –Galas

A. Część publiczna Polityki Bezpieczeństwa Danych Osobowych

§1

Podział Polityki Bezpieczeństwa Danych Osobowych

Wprowadza się podział Polityki Bezpieczeństwa Danych Osobowych (w skrócie PBDO), na:

A. część publiczną - dostępną dla zainteresowanych stron,
B. część niepubliczną - wewnętrzną, dostępną wyłącznie dla osób upoważnionych przez Administratora Danych Osobowych.

§2

Definicje

Szkoła - Szkoła Podstawowa nr 3 Przymierza Rodzin **im. bł. ks. Jerzego Popiełuszki w Warszawie przy ul. Nocznickiego 7. Kontakt tel.: (22) 864-92-50, adres e-mail:** sekretariat@spr3bielany.edu.pl**.**

Polityka Bezpieczeństwa Danych Osobowych (w skrócie Polityka, Polityka Bezpieczeństwa, PBDO) - niniejszy dokument określający nadrzędne zasady ochrony danych osobowych w Szkole.

Administrator Danych Osobowych (w skrócie ADO) - Szkoła przetwarzająca dane osobowe, określająca ich cel i sposoby przetwarzania.

Podmiot Przetwarzający (w skrócie Procesor) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora (Szkoły).

Inspektor Ochrony Danych (w skrócie IOD) - wyznaczona przez ADO osoba fizyczna pełniąca funkcję pełnomocnika ds. ochrony danych osobowych wpisana do rejestru właściwego Urzędu ds. ochrony danych osobowych.

Rozporządzenie (w skrócie 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).

Dane Osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dostępność – rozumie się przez to właściwość zapewniającą, że upoważnieni użytkownicy mają dostęp do informacji w każdej sytuacji, kiedy jest to niezbędne do realizacji ich zadań.

Poufność - rozumie się przez to właściwość zapewniającą, że dane osobowe są dostępne wyłącznie dla upoważnionych do tego osób, przy zachowaniu rozliczalności i integralności tych danych.

Rozliczalność - rozumie się jako właściwość zapewniająca, że działania podmiotu (osoby) mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (tej osobie).

Integralność - rozumie się jako właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Kodeks Ochrony Danych Osobowych (w skrócie KODO) - Kodeks ochrony danych osobowych stworzony przez Polskie Centrum Certyfikacji Bezpieczeństwa Informacji i Ochrony Danych Osobowych Sp. z o.o. z dnia 31.12.2017 r. (z późniejszymi zmianami).

Postać elektroniczna danych - dane przetwarzane za pomocą środków elektronicznych z formie zapisów w pamięci ulotnej i/lub stałej przetwarzane za pomocą Systemu Informatycznego.

Postać tradycyjna danych - dane w formie papierowej, przetwarzane za pomocą tradycyjnych metod składowania.

System Informatyczny - zbiór urządzeń teleinformatycznych wraz z zainstalowanym oprogramowaniem, i/lub systemem operacyjnym, pracujący jako całość i służący do przetwarzania danych.

Instrukcja Kancelaryjna (w skrócie IK) - dokument określający zasady przetwarzania danych osobowych w postaci tradycyjnej.

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.

Przetwarzanie danych osobowych (w skrócie Przetwarzanie) – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.

Naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§3

Cel i zakres polityki

1. Celem Polityki Bezpieczeństwa Danych Osobowych jest określenie kierunków działań oraz wsparcia dla zapewnienia bezpieczeństwa przetwarzania zbiorów danych osobowych zarządzanych przez Szkołę dla wykazania zgodności z wymogami RODO oraz innymi regulacjami prawnymi i wewnętrznymi wytycznymi dotyczącymi przetwarzania danych osobowych.

2. Przez bezpieczeństwo Danych Osobowych rozumie się zapewnienie ich poufności, integralności i dostępności oraz zapewnienie rozliczalności działań, zgodnie z Polityką Bezpieczeństwa.

3. Szkoła zarządza bezpieczeństwem danych osobowych w celu zapewnienia sprawnego i zgodnego z przepisami prawa wykonywania swoich zadań oraz zadań wykonywanych na podstawie umów lub zadań powierzonych do wykonania na podstawie innych porozumień.

4. Zakres przedmiotowy stosowania Polityki Bezpieczeństwa obejmuje wszystkie zbiory danych osobowych przetwarzanych w Szkole. W zakresie podmiotowym, Polityka Bezpieczeństwa obowiązuje wszystkich pracowników Szkoły oraz inne osoby mające dostęp do danych osobowych, w tym: stażystów, osoby zatrudnione na umowę zlecenia lub umowę o dzieło itp.

5. Niniejszą Politykę Bezpieczeństwa stosuje się do:
    a. danych osobowych przetwarzanych obecnie lub w przyszłości w systemie informatycznym,
    b. danych osobowych przetwarzanych obecnie lub w przyszłości w sposób tradycyjny.

6. Za realizację obowiązków wskazanych w niniejszej Polityce odpowiedzialny jest Administrator Danych Osobowych (ADO).

7. ADO wyznacza do pełnienia funkcji Inspektora Ochrony Danych Pana: Grzegorza Grabowskiego, e-mail: iod@pccbiodo.pl.

§4

Źródło wymagań

1. 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),

2. Ustawa o ochronie danych osobowych z 10 maja 2018 r. (Dz.U.2018.0.1000, z późn. zm.),

3. Kodeks Ochrony Danych Osobowych stworzony przez Polskie Centrum Certyfikacji Bezpieczeństwa Informacji i Ochrony Danych Osobowych Sp. z o. o. z dnia 31.12.2017 r (z póź. zm.),

4. Zasady i standardy określone przez Polską Normę PN-ISO/IEC 29151:2017.

§5

Deklaracja stosowania

1. ADO deklaruje w formie pisemnej, dostępnej na stronie www pod adresem: http://www.spr3bielany.edu.pl/index.php, że stosuje wszystkie opisane w niniejszej polityce zabezpieczenia organizacyjne i techniczne do ochrony danych osobowych.

2. Wersja tradycyjna deklaracji, jest dostępna w Szkole, w formie publicznego obwieszczenia.

3. Za deklarację stosowania przyjmuje się również publiczne udostępnienie wersji elektronicznej lub tradycyjnej, certyfikatu zgodności wystawionego przez Polskie Centrum Certyfikacji Bezpieczeństwa Informacji i Ochrony Danych Osobowych Sp. z o.o.

§6

Ogólne zasady bezpieczeństwo danych osobowych

1. ADO przetwarza dane osobowe w imieniu własnym jako ich Administrator, a także może je przetwarzać w imieniu Administratora jako Podmiot Przetwarzający oraz w przypadku wspólnie ustalonych celów i sposobów przetwarzania z innym podmiotem, jako współadministrator.

2. Przetwarzane dane osobowe są zabezpieczone zgodnie z Kodeksem Ochrony Danych Osobowych Polskiego Centrum Certyfikacji Bezpieczeństwa Informacji i Ochrony Danych Osobowych Sp. z o. o., w szczególności w zakresie:
    a. poufności,
    b. dostępności,
    c. integralności,
    d. i rozliczalności.

3. W powyższym zakresie zastosowano zabezpieczenia organizacyjne i techniczne m. in.:
    a. zatwierdzono i przyjęto niniejszą Politykę,
    b. zatwierdzono i przyjęto Instrukcję Zarządzania Systemem Informatycznym,
    c. oszacowano ryzyko w procesie przetwarzania danych osobowych,
    d. dopasowano odpowiednio zabezpieczenia techniczne, w szczególności w zakresie,
        i. ochrony przed nieautoryzowanym dostępem,
        ii. ochrony antywirusowej,
        iii. wykonywania kopii bezpieczeństwa,
        iv. szyfrowania dostępu do danych osobowych,
        v. ewidencjonowania incydentów i zdarzeń,
    e. wdrożono cykliczne szkolenia dla pracowników Szkoły,
    f. wdrożono cykliczne audyty wewnętrzne,
    g. wdrożono cykliczne audyty zewnętrzne, przystąpiono do procesu certyfikacji i uzyskano certyfikat zgodności Polskiego Centrum Certyfikacji Bezpieczeństwa Informacji i Ochrony Danych Osobowych Sp. z o. o.
4. Dane osobowe są przetwarzane:
    a. zgodnie z prawem, rzetelnie i w sposób przejrzysty,
    b. w sprecyzowanych, wyraźnie i prawnie uzasadnionych celach,
    c. tylko w takim zakresie, jaki jest niezbędny dla osiągnięcia celu ich zbierania,
    d. w formie aktualnej, umożliwiającej identyfikację osoby, przez czas niezbędny dla realizacji celu ich zbierania, a w razie potrzeby są uaktualniane, aby dane nieprawidłowe zostały usunięte lub sprostowane,
    e. w formie umożliwiającej identyfikację osoby, której dane dotyczą przez ograniczony okres, nie dłuższy, niż jest to niezbędne do celów, w których dane są przetwarzane,
    f. w sposób zapewniający odpowiednie bezpieczeństwo przed ich nieuprawnioną zmianą czy zniszczeniem,
    g. w sposób umożliwiający wykazanie przestrzegania powyższych zasad.

5. Administrator Danych Osobowych nie przetwarza tzw. szczególnych kategorii danych (o których mowa w art. 9 ust. 1 RODO)

6. Do wszystkich danych osobowych, niezależnie od ich kategorii, stosowane są w Szkole odpowiednie środki bezpieczeństwa.

7. ADO może wyznaczyć Administratora Systemu Informatycznego – informatyka odpowiedzialnego za zapewnienie ciągłości i bezpieczeństwa funkcjonowania Systemu Informatycznego, w szczególności do nadawania oraz odbierania uprawnień w imieniu ADO w Systemie Informatycznym.

8. ADO nadaje upoważnienia i dostęp do przetwarzania danych osobowych wyłącznie tym osobom, które zapoznały się z zasadami bezpieczeństwa i ochrony danych osobowych a także zobowiązały się do ich przestrzegania.

9. Dostęp do danych osobowych realizowany jest wyłącznie na podstawie ważnych upoważnień, dokładnie precyzujących zakres danych, czynności i cel ich przetwarzania.

10. ADO prowadzi ewidencję i monitoring upoważnień w sposób ciągły.

11. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zachowania w tajemnicy zasad ochrony danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskały dostęp w trakcie zatrudnienia jak również po jego ustaniu.

§7

Proaktywne podejście do ochrony danych

1. ADO kieruje się zasadami bezpieczeństwa określonymi w niniejszej Polityce do wszystkich rejestrów i zbiorów na etapie ich planowania i tworzenia uwzględniając przy tym ryzyko utraty i szacując zagrożenia wynikające z ich ujawnienia.

2. ADO do określenia ryzyka i zasadności zabezpieczeń organizacyjnych i technicznych stosuje metodykę opisaną w części B Polityki i stosuje zabezpieczenia tak, aby skutecznie chronić przetwarzane dane osobowe.

§8

Podstawa prawna przetwarzania danych osobowych

1. Jeżeli Administrator Danych Osobowych nie przetwarza danych osobowych bezpośrednio:

    a. na podstawie przepisów prawa polskiego,
    b. na podstawie przepisów prawa UE,
    c. na podstawie uzasadnionego interesu,
    d. w ramach wykonywania umowy,
    e. w celu ochrony żywotnych interesów,
    f. lub wykonując zadanie realizowane w interesie publicznym,

    to podstawą przetwarzania tych danych jest zgoda uzyskana od właściciela danych.

2. Zgoda wyrażana jest samodzielnie, świadomie i dobrowolnie na podstawie oświadczenia, w formie tradycyjnej lub elektronicznej. Formuła zgody jest przedstawiona przejrzyście i

przystępnie dla każdej osoby fizycznej odpowiednio do jej wieku. Każda zgoda zawiera ponadto, zakres i cel przetwarzania danych.

3. W procesie uzyskiwania danych osobowych ADO wypełnia swój obowiązek informacyjny rzetelnie i przy zachowaniu profesjonalnego charakteru swojej działalności.

§9

Prawo dostępu do danych

1. Administrator Danych Osobowych umożliwia dostęp do przetwarzanych danych osobowych każdemu właścicielowi danych na podstawie złożonego wniosku. Po potwierdzeniu tożsamości, kopia danych udostępniona jest za pomocą tego samego kanału, przez który wpłynął wniosek: elektronicznie lub drogą tradycyjną.

2. ADO ma prawo odmówić dostępu do części lub całości danych, które są przetwarzane w przypadku, gdy wniosek jest nieuzasadniony lub w przypadku nadmiernego stosowania tego prawa.

3. W przypadku, gdy ADO odmówił dostępu do danych, wskazuje powody odmowy i w tej samej formie, w której otrzymał wniosek, informuje o swojej odmowie. ADO przekazuje wnioskodawcy informację o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

§10

Prawo poprawiania danych

1. Administrator Danych Osobowych umożliwia poprawianie właścicielowi swoich danych osobowych na podstawie złożonego wniosku. Po potwierdzeniu tożsamości, dane są modyfikowane a informacja o tym jest udzielana za pomocą tego samego kanału, przez który wpłynął wniosek: elektronicznie lub drogą tradycyjną.

2. ADO ma prawo odmówić modyfikacji części lub całości danych, które są przetwarzane w przypadku, gdy wniosek jest nieuzasadniony lub w przypadku nadmiernego stosowania tego prawa.

3. W przypadku, gdy ADO odmówił modyfikacji danych, wskazuje powody odmowy i w tej samej formie, w której otrzymał wniosek, informuje o swojej odmowie. ADO przekazuje wnioskodawcy informację o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

§11

Prawo do bycia zapomnianym

1. Administrator Danych Osobowych umożliwia właścicielowi usunięcie swoich danych osobowych ze wszystkich rejestrów ADO na podstawie złożonego wniosku. Po potwierdzeniu tożsamości, w przeciągu 30 dni dane są usuwane a informacja o tym jest udzielana za pomocą tego samego kanału, przez który wpłynął wniosek: elektronicznie lub drogą tradycyjną.

2. Usunięcie danych nastąpi zgodnie z zasadami i procedurami opisanymi w Instrukcji Zarządzania Systemem Informatycznym, a jeżeli dane są przetwarzane w formie papierowej, zgodnie z Instrukcją Kancelaryjną.

3. ADO ma prawo odmówić usunięcia części lub całości danych, które są przetwarzane w przypadku, gdy wniosek jest nieuzasadniony lub w przypadku, w którym przepisy prawa polskiego lub UE nakazują zachowanie takich danych.

4. W przypadku, gdy ADO odmówił usunięcia danych, wskazuje powody odmowy i w tej samej formie, w której otrzymał wniosek, informuje o swojej odmowie. ADO przekazuje wnioskodawcy informację o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

§12

Prawo do sprzeciwu

1. Administrator Danych Osobowych umożliwia właścicielowi danych osobowych wyrażenie sprzeciwu w zakresie przetwarzania części lub całości swoich danych osobowych. ADO biorąc pod uwagę indywidualną sytuację i konkretne dane, po potwierdzeniu tożsamości, przyjmuje sprzeciw a informacja o tym udzielana jest za pomocą tego samego kanału, przez który wpłynął wniosek: elektronicznie lub drogą tradycyjną.

2. Dane Osobowe dla których wniesiono skutecznie sprzeciw nie są wykorzystywane ani przetwarzane przez Administratora Danych Osobowych. Jeżeli wykorzystanie danych jest niezbędne ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej, ADO ma obowiązek udowodnienia, że przetwarzanie przez niego tych danych jest konieczne i prawnie uzasadnione.

3. W przypadku, gdy ADO odmówił realizacji sprzeciwu, wskazuje powody odmowy i w tej samej formie, w której otrzymał wniosek, informuje o swojej odmowie. ADO przekazuje wnioskodawcy informację o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

§13

Prawo do przenoszenia danych

1. Administrator Danych Osobowych umożliwia właścicielowi przeniesienie swoich danych osobowych do innego (wskazanego) podmiotu (innego administratora danych osobowych) na podstawie złożonego wniosku. Po potwierdzeniu tożsamości, w przeciągu 30 dni dane są przekazywane a informacja o tym jest udzielana za pomocą tego samego kanału, przez który wpłynął wniosek: elektronicznie lub drogą tradycyjną.

2. Przekazanie danych nastąpi zgodnie z zasadami i procedurami opisanymi w Instrukcji Zarządzania Systemem Informatycznym, a jeżeli dane są przetwarzane w formie papierowej, zgodnie z Instrukcją Kancelaryjną. Forma przekazania danych uzależniona jest od możliwości technicznych ADO. W zależności od zawartości wniosku o przeniesienie a także w zależności od obowiązków prawnych, dane osobowe osoby przenoszonej zostaną zachowane lub usunięte z rejestrów ADO.

3. ADO ma prawo odmówić przekazania części lub całości danych, które są przetwarzane w przypadku, gdy wniosek jest nieuzasadniony lub w przypadku, w którym przepisy prawa polskiego lub UE nakazują zachowanie takich danych.

4. W przypadku, gdy ADO odmówił przekazania danych, wskazuje powody odmowy i w tej samej formie, w której otrzymał wniosek, informuje o swojej odmowie. ADO przekazuje wnioskodawcy informację o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

5. Administrator danych, niezależnie od informacji zawartych w §9-§13, celem realizacji praw osób, których dane dotyczą, może stosować wewnętrzne procedury celem spełnienia żądań tych osób, nie uchybiając przepisom RODO.

§14

Udostępnienie i powierzanie danych osobowych

1. W przypadku uzasadnionej potrzeby lub konieczności powierzenia danych osobowych przetwarzanych w sposób elektroniczny lub tradycyjny, do podmiotu, który ma realizować cele wskazane przez ADO, zawierana jest umowa powierzenia przetwarzania.

2. Powierzenie danych może nastąpić o ile podmiot, któremu dane są powierzane:
   a. posiada wdrożone środki bezpieczeństwa ochrony danych osobowych co najmniej na takim samym poziomie co środki Administratora Danych Osobowych

   lub

   b. posiada ważny certyfikat Polskiego Centrum Certyfikacji Bezpieczeństwa Informacji i Ochrony Danych Osobowych Sp. z o.o.

   lub

   c. posiada inny certyfikat bezpieczeństwa (informacji lub danych osobowych) wystawiony przez uznany na rynku polskim lub UE podmiot

   lub

   d. udzieli pisemnych gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych by przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.

§15

Prawo do wniesienia skargi do organu nadzorczego

1. Każda osoba fizyczna, której dane osobowe przetwarza ADO, ma prawo wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych, jeśli uważa, że jego dane są przetwarzane niezgodnie z prawem.

2. Administrator Danych Osobowych dostosuje cel i zakres przetwarzania danych do prawnie wiążącej decyzji tego organu bez zbędnej zwłoki w czasie nie dłuższym niż 30 dni.

3. Każda osoba fizyczna może w tej sprawie występować osobiście, jak również ma możliwość do umocowania innego podmiotu, organizacji czy zrzeszenia – do przemawiania w jej imieniu.

§16

Naruszenie ochrony danych osobowych

1. W przypadku pozyskania informacji z jakiegokolwiek źródła o potencjalnym naruszeniu ochrony danych osobowych, Administrator Danych Osobowych natychmiast podejmuje niezbędne środki w celu ustalenia, czy konkretne zdarzenie miało miejsce, a następnie, czy stanowiło ono naruszenie ochrony danych osobowych.

2. Uwzględniając zakres i charakter takiego naruszenia, ADO podejmuje działania, które ograniczą rozmiar i dotkliwość naruszenia dla osób, których danych ono dotyczyło. W szczególności realizowana jest klasyfikacja naruszenia i szacowanie zagrożeń dla osób fizycznych zgodnie z przyjętą metodyką opisaną w części B.

3. W przypadku stwierdzenia wystąpienia naruszenia ochrony danych osobowych Administrator Danych Osobowych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po jego stwierdzeniu, zgłasza je Prezesowi Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Po upływie 72 godzin dołącza się wyjaśnienia przyczyn opóźnienia.

4. ADO biorąc pod uwagę swoje możliwości techniczne a także zagrożenie, mogące powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, wynikające z zaistnienia incydentu, poinformuje o tym fakcie właścicieli danych osobowych.

5. Wszelkie naruszenia ochrony danych osobowych oraz sytuacje nie stanowiące takiego naruszenia, będące jednak incydentem w zakresie ochrony danych, są dokumentowane przez ADO, zgodnie z przyjętą metodyką.

§17

Monitorowanie i sprawdzanie

1. Administrator Danych Osobowych przestrzegając zasad certyfikacji Polskiego Centrum Certyfikacji Bezpieczeństwa Informacji i Ochrony Danych Osobowych Sp. z o.o.:
    a. co najmniej raz na 6 miesięcy:
        i. zarządza przegląd polityk, zasad i procedur ochrony danych osobowych,
        ii. jeżeli uzna za zasadne, przeprowadza ponowne określenie i szacowanie ryzyka,
        iii. przegląda stan zabezpieczeń systemów teleinformatycznych,
    b. co najmniej raz na 12 miesięcy:
        i. podnosi świadomość wszystkich pracowników i wzmacnia ich zaangażowanie w ochronę danych osobowych np. poprzez przeprowadzenie szkolenie przypominającego z ochrony danych osobowych,
        ii. przystępuje do procesu audytu kontrolnego w celu recertyfikacji.

Dyrektor

Mirosława Piasecka –Galas

01.04.2019r