AKTUALIZACJA POLITYKI OCHRONY DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ NR 6 W BĘDZINIE

1. WPROWADZENIE

Niniejsza Aktualizacja Polityki Ochrony Danych Osobowych została stworzona w związku z wymaganiami, które stawia przed Administratorami danych osobowych oraz Podmiotami przetwarzającymi Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne Rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1), zwane dalej RODO oraz Ustawia z dnia 10 maja 2018 r. o ochronie danych osobowych oraz wydanych na jej podstawie Rozporządzeń.

Celem niniejszej Aktualizacji Polityki Ochrony Danych Osobowych jest odpowiednie dostosowanie istniejącego już dokumentu Polityki Bezpieczeństwa posiadanego przez Administratora do zmian, jakie zostały narzucone przez RODO oraz do Ustawy o Ochronie Danych Osobowych jak i do zasad ochrony danych osobowych wdrożonych w Placówce.

Niniejszy dokument dotyczy wszystkich przetwarzanych przez Szkołę Podstawową nr 6 danych osobowych, niezależnie od formy ich przetwarzania (tradycyjnej lub w systemach informatycznych).

Postanowienia niniejszej Polityki Ochrony Danych Osobowych dotyczą wszystkich pracowników, współpracowników, a także osób bądź podmiotów, którym powierzane są dane osobowe na podstawie umowy powierzenia danych. Ponadto Polityka Ochrony Danych Osobowych opisuje granice dopuszczalnego zachowania, opisuje konsekwencje ich przekraczania, procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano obowiązki leżące po stronie Administratora danych. Niniejszy Dokument sporządzony został w formie pisemnej i przechowywana jest w formie tradycyjnej oraz elektronicznej w siedzibie Administratora danych osobowych.

Niniejsza Aktualizacja jest udostępniania do wglądu wszystkim osobom upoważnionym do przetwarzania danych osobowych w pokoju nauczycielskim, a także osobom, którym takie upoważnienie ma dopiero zostać nadane, celem zapoznania się z jej treścią.

Wszystkie osoby przed rozpoczęciem przetwarzania danych osobowych w Placówce mają obowiązek zapoznania się z Polityką Bezpieczeństwa oraz jej Aktualizacją oraz zobowiązania się do przestrzegania ich zapisów.

Dokument ten stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

2. DEFINICJE

Polityka Ochrony Danych Osobowych (Polityka) – niniejsza Polityka, o ile z kontekstu nie wynika inaczej.

Dane Osobowe – są to dane o zidentyfikowanej, bądź możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą).

Dane osobowe szczególnej kategorii - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Osoba fizyczna - to prawne określenie człowieka, jako podmiotu stosunku cywilnoprawnego. Osoba fizyczna rozpoczyna swój byt prawny w chwili urodzenia, a kończy go w chwili śmierci. Osoby fizyczne posiadają zdolność prawną, a także po spełnieniu określonych warunków zdolność do czynności prawnych.

Osoba możliwa do zidentyfikowania – to osoba fizyczna, którą można pośrednio lub bezpośrednio zidentyfikować, w szczególności za pomocą identyfikatora takiego jak imię, nazwisko, nr identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Administrator Danych Osobowych (ADO) - jest decydentem w procesie przetwarzania danych osobowych. Decyduje o sposobie i celu przetwarzania danych.

Inspektor Ochrony Danych Osobowych (IOD) – to osoba powołana przez Administratora celem informowania o obowiązkach wynikających z przepisów prawa o ochronie danych osobowych, w tym RODO, nadzoru nad przestrzeganiem tych przepisów, zarządzania ryzykiem, współpracy z organami nadzorczymi oraz osobami, których dane dotyczą.

Prezes Urzędu Ochrony Danych Osobowych – Prezes Urzędu jest organem nadzorczym w rozumieniu 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 (Dziennik Urzędowy UE - 4.5.2016 L 119/3).

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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).

Ustawa – Ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku (Dz. U. 2018 poz. 1000).

RCPD (Rejestr czynności) - oznacza Rejestr Czynności Przetwarzania Danych Osobowych, stosowany przez Administratora.

RKCPD (Rejestr kategorii) - oznacza Rejestr Kategorii Czynności Przetwarzania Danych Osobowych, stosowany przez podmiot przetwarzający.

Aktywa – są to środki materialne i niematerialne mające wpływ na przetwarzanie danych (np. systemy informatyczne, zasoby ludzkie).

Przetwarzanie danych osobowych - 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.

Ochrona danych osobowych - dołożenie wszelkich starań celem zabezpieczenia danych osobowych osoby, której dane dotyczą poprzez zapewnienie szczególnych środków technicznych i organizacyjnych do ochrony danych. Zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Ręczne przetwarzanie danych osobowych – przetwarzanie danych osobowych z pominięciem systemów informatycznych (forma tradycyjna, papierowa).

Zautomatyzowane przetwarzania danych osobowych – przetwarzanie danych osobowych w systemach informatycznych bez udziału człowieka (np. automatyczne podejmowanie decyzji).

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Profilowanie - polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą.

Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Osoba uprawniona do przetwarzania danych osobowych - jest to osoba posiadające pisemne upoważnienie do przetwarzania danych osobowych nadane przez Administratora danych osobowych.

Zgoda na przetwarzanie danych osobowych – jest to dobrowolne, sprecyzowane, świadome i jednoznaczne określenie woli osoby, której dane dotyczą, wyrażone w formie pisemnego oświadczenia złożonego na formularzu w formie tradycyjnej lub przesłanego za pośrednictwem poczty elektronicznej.

Podmiot przetwarzający dane osobowe (procesor) – osoba fizyczna lub prawna, organy publiczne, jednostki lub inne podmioty przetwarzające dane osobowe w imieniu Administratora i w jego interesie. Realizuje jego cele, świadcząc mu usługi związane z powierzeniem mu przetwarzania danych osobowych. Nie decyduje o celach

i środkach ochrony danych osobowych, działa w interesie Administratora i na wyraźne jego polecenie. Z takimi podmiotami podpisuje się umowę powierzenie przetwarzania danych osobowych.

Zbiór danych osobowych - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Ryzyko - to możliwość zaistnienia zdarzenia, które może mieć wpływ na realizację założonych celów w zakresie ochrony danych osobowych. Ryzyko mierzone jest siłą skutku oddziaływania oraz prawdopodobieństwem jego wystąpienia.

Zarządzanie ryzykiem - jest to kilkuetapowy proces polegający na wyszukaniu i nazwaniu każdego ryzyka zagrażającego danym przetwarzanym przez Administratora wraz ze źródłami, przyczynami i wstępnym określeniem szkód jakie im towarzyszą. Następnie na szacowaniu prawdopodobieństwa wystąpienia zdefiniowanych rodzajów ryzyka, określenie wartości prawdopodobnych strat, a następnie minimalizacja tych ryzyk.

Ocena ryzyka – jest to zespół czynności polegających na ocenie prawdopodobieństwa wystąpienia niepożądanych zdarzeń związanych z ochrona danych osobowych. Ocena ryzyka opiera się o szczegółową analizę ryzyka.

Bezpieczeństwo informacji – polega na zapewnieniu bezpieczeństwa informacji, poprzez określenie ogółu zasad, metod i narzędzi ochrony i nadzoru nad informacją. Narzędzia te powinny być budowane w taki sposób aby zapewnić poufność, autentyczności, dostępność, integralność danych oraz systemów, rozliczalności oraz niezawodność.

Incydent (naruszenie zasad ochrony danych osobowych) - to incydent polegający na przypadkowym lub niezgodnym z prawem modyfikowaniu, niszczeniu, utracie danych, nieuprawnionym ujawnieniu ich treści lub nieuprawnionym dostępie do danych osobowych.

Zagrożenie - są to czynnymi zewnętrzne lub wewnętrzne mogące prowadzić do wystąpienia incydentu i mogące mieć negatywny wpływ na proces przetwarzania danych osobowych.

Podatność – jest to potencjalnie słaby punkt (luka w bezpieczeństwie), który może być wykorzystany przez zagrożenie, doprowadzając do negatywnych skutków.

Integralność – to właściwość oznaczająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany. A w przypadku systemów informatycznych, właściwość umożliwiająca systemowi realizację zamierzonej funkcji w nienaruszony przez nieautoryzowane manipulacje (celowe lub przypadkowe) sposób.

Informatyczny nośnik danych – jest to urządzenie służące do zapisu, przechowywania i odczytu danych osobowych (np. płyta CD, DVD, pendrive, dysk, itp.).

Zasoby systemu teleinformatycznego – są to wszystkie dane zgromadzone w systemach informatycznych, jak również, sprzęt, oprogramowanie czy użytkownicy.

Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

3. ZAGADNIENIA DOTYCZĄCE OCHRONY DANYCH OSOBOWYCH

Informacja dotycząca zmiany nazewnictwa w związku z wejściem w życie nowych przepisów dotyczących ochrony danych osobowych

Od 25 maja 2018 roku urząd Generalnego Inspektora Ochrony Danych Osobowych (GIODO) zmienił nazwę na Prezesa Urzędu Ochrony Danych Osobowych (PUODO), Biuro Generalnego Inspektora Ochrony Danych Osobowych stało się natomiast Urzędem Ochrony Danych Osobowych.

Z mocy prawa dotychczasowy Generalny Inspektor, została Prezesem nowopowstałego Urzędu Ochrony Danych Osobowych. Zmianie uległy nie tylko nazwa, ale znacznie więcej.

Celem zmian było odróżnienie etapów prawnej ochrony danych osobowych i wyróżnienie nowych, jednolitych dla całej Unii Europejskiej standardów. Głównym celem polskiego ustawodawcy było natomiast uporządkowanie krajowej nomenklatury związanej z funkcjami pełnionymi w systemie ochrony danych osobowych.

RODO wprowadziło funkcję Inspektora Ochrony Danych (IOD), która zastąpiła dotychczasową funkcję Administratora Bezpieczeństwa Informacji (ABI). Dalsze posługiwanie się przez organ odpowiedzialny za ochronę danych osobowych w Polsce nazwą Generalny Inspektor Ochrony Danych Osobowych (GIODO) mogłoby sugerować powiązanie pomiędzy GIODO a powoływanymi przez Administratorów danych Inspektorami Ochrony Danych (IOD) i wprowadzać tym samym w błąd.

Ustawodawca zmienił także nazwę dotychczasowych inspektorów dokonujących kontroli z ramienia GIODO na pracowników Urzędu Ochrony Danych Osobowych.

Z Rozporządzenia Parlamentu Europejskiego i Rady wynika, iż osoby powołane przez Administratorów Danych do pełnienia funkcji IOD są niezależne od pełniącego obowiązki PUODO.

Wraz ze zmianą nazewnictwa zmienił się także zakres kompetencji IOD oraz PUODO.

Prezes Urzędu Ochrony Danych Osobowych (PUODO)

Prezes Urzędu Ochrony Danych Osobowych jako organ nadzorczy w rozumieniu Rozporządzenia:

- monitoruje i egzekwuje stosowanie Rozporządzenia Parlamentu Europejskiego i Rady;
- upowszechnia w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk. Szczególną uwagę poświęca działaniom skierowanym do dzieci;
- doradza, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem;
- upowszechnia wśród Administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy RODO;
- udziela osobie, której dane dotyczą, na jej żądanie, informacji o wykonywaniu praw przysługujących im na mocy Rozporządzenia, a w stosownym przypadku współpracuje w tym celu z organami nadzorczymi innych państw członkowskich;
- rozpatruje skargi wniesione przez osobę, której dane dotyczą, lub przez podmiot, organizację lub zrzeszenie zgodnie z art. 80 Rozporządzenia, w odpowiednim zakresie prowadzi postępowania w przedmiocie tych skarg i w rozsądnym terminie informuje skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowań lub koordynacja działań z innym organem nadzorczym;
- współpracuje z innymi organami nadzorczymi, w tym dzieli się informacjami oraz świadczy wzajemną pomoc, w celu zapewnienia spójnego stosowania i egzekwowania RODO;
- prowadzi postępowania w sprawie stosowania Rozporządzenia, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego;
- monitoruje zmiany w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitoruje rozwój technologii informacyjno-komunikacyjnych i praktyk handlowych;
- przyjmuje standardowe klauzule umowne, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d. Rozporządzenia;

- ustanawia i prowadzi wykaz związany z wymogiem dokonania oceny skutków dla ochrony danych na mocy art. 35 ust. 4 Rozporządzenia;
- udziela zaleceń, o których mowa w art. 36 ust. 2 Rozporządzenia, dotyczących operacji przetwarzania;
- zachęca do sporządzania kodeksów postępowania zgodnie z art. 40 ust. 1 Rozporządzenia, wydaje opinie na ich temat oraz zatwierdza te kodeksy, w których znajdują się odpowiednie zabezpieczenia, na mocy art. 40 ust. 5 Rozporządzenia;
- zachęca do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń z tej dziedziny zgodnie z art. 42 ust. 1 Rozporządzenia, a także zatwierdza kryteria certyfikacji zgodnie z art. 42 ust. 5 Rozporządzenia;
- gdy ma to zastosowanie – zgodnie z art. 42 ust. 7 Rozporządzenia dokonuje okresowego przeglądu udzielonych certyfikacji;
- opracowuje i publikuje kryteria akredytacji podmiotu monitorującego kodeksy postępowania na mocy art. 41 Rozporządzenia oraz podmiotu certyfikującego na mocy art. 43 Rozporządzenia;
- akredytuje podmiot monitorujący kodeksy postępowania na mocy art. 41 Rozporządzenia oraz podmiot certyfikujący na mocy art. 43 Rozporządzenia;
- wydaje zezwolenia na klauzule umowne i przepisy, o których mowa w art. 46 ust. 3 Rozporządzenia;
- zatwierdza wiążące reguły korporacyjne na mocy art. 47 Rozporządzenia;
- bierze udział w pracach Europejskiej Rady Ochrony Danych;
- prowadzi wewnętrzny rejestr naruszeń RODO i działań podjętych zgodnie z art. 58 ust. 2 Rozporządzenia;
- wypełnia inne zadania związane z ochroną danych osobowych.

Kontrole PUODO

Kontrolę przeprowadza upoważniony przez Prezesa Urzędu Ochrony Danych Osobowych:

- pracownik Urzędu,
- członek lub pracownik organu nadzorczego państwa członkowskiego Unii Europejskiej w przypadku, o którym mowa w art. 62 Rozporządzenia – zwany dalej „kontrolującym".

Kontrolujący ma prawo:

- wstępu w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń;

- wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;
- przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
- żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;
- zlecać sporządzanie ekspertyz i opinii.

Działania PUODO w przypadku naruszenie przepisów:

Jeżeli na podstawie informacji zgromadzonych w postępowaniu kontrolnym Prezes Urzędu Ochrony Danych Osobowych uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania w sprawie naruszenia przepisów o ochronie danych osobowych.

Inspektor Ochrony Danych (IOD)

Zgodnie z art. 37 ust. 1 pkt RODO Administrator Danych Osobowych powołuje Inspektora Ochrony Danych (IOD).

Do jego obowiązków należy:

- Informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- Monitorowanie przestrzegania oraz polityk 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;
- Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
- Współpraca z organem nadzorczym;
- Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

- Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego Rozporządzenia.

Przetwarzanie danych

Przetwarzanie **danych zwykłych**

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Przetwarzanie **danych szczególnych kategorii**

Przetwarzanie danych jest **zabronione** w przypadku danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Przetwarzanie tych danych **jest jednak dopuszczalne**, jeżeli:

- osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego

przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania danych szczególnych;

- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

- przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

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

- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową
  z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 9 ust. 3 Rozporządzenia;

- przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego,

które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

- przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

4. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Nowym i niezmiernie istotnym elementem Polityki Ochrony Danych, a także całego procesu zarzadzania danymi osobowymi przez Administratora Danych jest Rejestr Czynności Przetwarzania Danych Osobowych (RCPD) - **załącznik nr 1.** Identyfikuje on wszystkie procesy dotyczące danych osobowych zachodzące na wszystkich zbiorach, pozwala na kontrolę nad tymi procesami oraz systemami używanymi do ich realizacji.

RCPD stanowi formę dokumentowania czynności przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację jednej z głównych zasad opisanych w RODO, czyli zasady rozliczalności.

Administrator Danych Osobowych prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Rejestr czynności stanowi podstawowe narzędzie do rozliczenia wszystkich obowiązków ochrony danych.

W Rejestrze czynności, dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, odnotowuje się co najmniej:

- Określenie czynności przetwarzania/nazwa zbioru;
- Właściciel aktywów;
- Cel przetwarzania;
- Kategorie osób, których dane dotyczą;
- Kategorie danych osobowych;
- Podstawa prawna;
- Źródło pozyskania danych;
- Planowany termin usunięcia kategorii danych (lub kryterium określenia terminu);
- Nazwa współadministratora i dane kontaktowe (jeśli dotyczy);
- Nazwa podmiotu przetwarzającego i dane kontaktowe;

- Kategorie odbiorców (innych niż podmiot przetwarzający);
- Sposób przetwarzania/nazwa programu;
- Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie (art. 32 ust. 1 RODO);
- Ocena skutków dla ochrony danych;
- Transfer do kraju trzeciego lub organizacji międzynarodowej;
- Ewentualne środki zabezpieczeń poza EOG

W przypadku gdy Administrator danych występuje także w roli Podmiotu Przetwarzającego, na mocy umowy powierzenia przetwarzania danych osobowych, prowadzi on Rejestr Kategorii Czynności przetwarzania danych osobowych – **załącznik nr 2.**

5. ZGODNOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH Z PRAWEM

Administrator zgodnie z zasadą rozliczalności zapewnia, by dane osobowe przetwarzane były zgodnie z prawem, w sposób rzetelny i przejrzysty. Dane osobowe przetwarzane są w zakresie niezbędnym dla realizacji celów tego przetwarzania. Cele przetwarzania określane są w sposób wyraźny i konkretny, dalsze zaś przetwarzanie
w sposób niezgodny z tymi celami jest zabronione za wyjątkiem przypadków wskazanych w przepisach obowiązującego prawa, bądź po uzyskaniu zgody na przetwarzanie danych osobowych dla nowych celów. Dane osobowe są aktualne i prawidłowe i w razie potrzeby uaktualniane.
Dane osobowe przechowywane są przez oznaczony czas niezbędny dla zapewnienia realizacji celów przetwarzania lub do czasu przedawnienia ewentualnych roszczeń.

Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Administratora) Administrator określa podstawę w czytelny sposób, gdy jest to potrzebne np. w przypadku zgody wskazując na jej zakres, gdy podstawą jest przepis prawa – wskazując na konkretny przepis, dla uzasadnionego celu Administratora– wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

Administrator danych osobowych zapewnia wykonanie wobec osób, których dane dotyczą obowiązku informacyjnego zgodnie z art. 13 (w przypadku pozyskania danych od osoby, której dane dotyczą) i 14 (w przypadku pozyskania danych nie od osoby, której dane dotyczą) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 („RODO”), wskazując prawa przysługujące tym osobom w tym: prawa dostępu do danych osobowych, sprostowania, usunięcia tzw. prawo do „bycia zapomnianym”, ograniczenia przetwarzania, wniesienia sprzeciwu czy cofnięcia zgody na przetwarzanie danych osobowych. Osoby te informuje się również o tym, kto jest Administratorem ich danych osobowych, o powołanym Inspektorze Ochrony Danych oraz jego

danych kontaktowych. Administratora danych nie obejmuje obowiązek informowania osoby, której dane dotyczą w przypadku, gdy dane te muszą zostać objęte tajemnicą zawodową.

Wskazane wyżej informacje Administrator podaje do wiadomości osoby, której dane dotyczą:

1. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
2. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą;
3. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

Wzory stosowanych przez administratora klauzul obowiązku informacyjnego stanowią **załącznik nr 3** do niniejszej Aktualizacji.

Przy powierzaniu przetwarzania danych osobowych w imieniu Administratora, dokonuje on wyboru wyłącznie takich podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. W tym celu Administrator zawiera z podmiotami przetwarzającymi stosowne umowy powierzenia przetwarzania danych osobowych (art. 28 RODO). Wzór umowy powierzenia przetwarzania danych osobowych stanowi **załącznik nr 4**.

W przypadku stwierdzenia naruszeń lub możliwości naruszenia zasad ochrony danych osobowych, należy zastosować procedurę postępowania w przypadku naruszeń ochrony danych opisaną poniżej w punkcie 7.

6. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Do nadawania i anulowania upoważnień do przetwarzania danych osobowych zarówno w zbiorach papierowych jak i w systemach informatycznych uprawniony jest wyłącznie Administrator danych osobowych. Dane osobowe mogą być przetwarzane wyłącznie na jego polecenie bądź na podstawie przepisów obowiązującego prawa.

Przed wydaniem upoważnienia do przetwarzania danych osobowych, osoba mająca takie upoważnienie uzyskać ma obowiązek zapoznania się z aktualną Polityką Ochrony Danych Osobowych.

Upoważnienie wydane może być na czas określony lub do odwołania (wzór odwołania stanowi **załącznik nr 5** do niniejszej Polityki).

Upoważnienia określają zakres operacji na danych, jak również identyfikator upoważnianej osoby w systemie informatycznym. Upoważnienie wydawane jest jedynie w zakresie niezbędnym do wykonywania powierzonych

przez Administratora czynności przetwarzania danych osobowych. Zmiana zakresu upoważnienie wymaga ponownego nadania upoważnienie.

Wzór upoważnienia do przetwarzania danych osobowych stanowi **załącznik nr 6** do niniejszej Polityki. Prowadzona jest również ewidencja nadanych upoważnień, której wzór stanowi **załącznik nr 7**.

Pracownikom, którzy w ramach swoich obowiązków służbowych nie przetwarzają danych osobowych, Administrator danych osobowych wydaje zgody na przebywanie w obszarze przetwarzania danych osobowych. Wzór takiej zgody zamieszczono w **załączniku nr 8.**

Przetwarzanie danych osobowych przez podmioty przetwarzające odbywa się na podstawie udokumentowanego polecenia Administratora w postaci umowy powierzenia przetwarzania danych osobowych zawartej z podmiotem przetwarzającym. Wzór umowy powierzenia przetwarzania danych osobowych stanowi **załącznik nr 4**.

7. INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

Instrukcja określa katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych w Placówce oraz w jasny sposób pokazuje jak należy na nie reagować. Instrukcja na ma celu zminimalizowanie skutków wystąpienia naruszenia zasad ochrony danych osobowych oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

Każde naruszenie bądź podejrzenie naruszenia zasad ochrony danych osobowych powinno być niezwłocznie zgłaszane bezpośredniemu przełożonemu bądź bezpośrednio do Administratora danych osobowych.

Za **naruszenie lub próbę naruszenia zasad przetwarzania danych osobowych** w Placówce uznaje się:

- nieodpowiednie zabezpieczenie pomieszczeń, urządzeń lub dokumentów;
- niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
- naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe;
- uszkodzenie, utratę, zmianę, lub nieuprawnione kopiowanie danych osobowych;
- udostępnienie lub możliwość udostępnienia danych osobowych osobom nieuprawnionym;

- nieprzestrzeganie obowiązku ochrony przetwarzanych danych osobowych;
- niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczeń;
- przetwarzanie danych osobowych bez upoważnienia;
- przetwarzanie danych osobowych niezgodnie z ich zakresem lub celem zebrania;
- przetwarzanie danych osobowych poza obszarem przetwarzania danych osobowych bez wiedzy i zgody Administratora;
- naruszenie praw osób, których dane dotyczą;
- niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie na klucz pomieszczeń, szaf, biurek.

Typowymi incydentami bezpieczeństwa danych osobowych nazwać można:

- wszystkie nieprzewidziane zdarzenia losowe w obszarze przetwarzania danych osobowych, takie jak: pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;
- wszystkie zdarzenia losowe dotyczące sprzętów, takie jak: awarie serwera, komputerów, twardych dysków, pendrive'ów, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych, brak możliwości zalogowania się do systemu, zmiana wyglądu pulpitu komputera;
- umyślne incydenty takie jak: włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania, naruszenia ochrony danych osobowych przez osoby zatrudnione przy przetwarzaniu danych.

Każdorazowo po otrzymaniu informacji o zaistnieniu lub możliwości zaistnienia naruszenia zasad ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło spowodować ryzyko naruszenia praw lub wolności osoby fizycznej, której dane dotyczą. Czynności te ujęte są w raporcie z naruszenia bezpieczeństwa zasad ochrony danych osobowych – **załącznik nr 9.** W przypadku stwierdzenia wystąpienia naruszenia ochrony danych osobowych, Administrator lub IOD prowadzi postępowanie wyjaśniające w toku, którego:

- ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
- proponuje ewentualne działania zaradcze;
- zaleca szereg działań mających na celu przywrócenia prawidłowego działania organizacji po wystąpieniu incydentu;
- rekomenduje działania mające na celu zapobieganie podobnym incydentom w przyszłości lub zmniejszenie strat w momencie ich zaistnienia.

Administrator ewidencjonuje wszelkie powyższe naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, ich skutki oraz podjęte działania zaradcze w Rejestrze naruszeń ochrony danych osobowych – **załącznik nr 10.**

Jeżeli Administrator stwierdził możliwość wystąpienia na skutek incydentu ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, zgłasza fakt naruszenia ochrony danych osobowych do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki, jednakże nie później niż w ciągu 72 godzin od momentu stwierdzenia naruszenia. Zgłoszenia naruszenia dokonuje się elektronicznie za pomocą odpowiedniego formularza dostępnego na stronie internetowej Urzędu Ochrony Danych Osobowych: uodo.gov.pl. Formularz należy wypełnić a następnie załączyć do pisma ogólnego dostępnego na platformie biznes.gov.pl bądź wysłać przez elektroniczną skrzynkę podawczą ePUAP: /UODO/SkrytkaESP.

Jeżeli zaistniałe ryzyko naruszenia ochrony danych osobowych jest wysokie dla osoby, której dane dotyczą, Administrator informuje ją, wskazując jednocześnie w jaki sposób zagrożona osoba może podjąć próbę zapobieżenia negatywnym skutkom naruszenia dla jej wolności i praw.

Każdorazowe powiadomienie osoby, której dane osobowe zostały naruszone, powinno zawierać:

- Dane Administratora Danych Osobowych
- Dane IOD (osoba kontaktowa)
- Data i miejsce naruszenia
- Opis charakteru naruszenia ochrony danych osobowych
- Możliwe konsekwencje naruszenia ochrony danych osobowych
- Środki zastosowane w celu minimalizacji skutków naruszenia ochrony danych osobowych
- Rekomendacja dla osoby zagrożonej

Zabrania się świadomego wywoływania incydentów przez wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w Placówce.

8. ANALIZA RYZYKA I OCENA SKUTKÓW DLA OCHRONY DANYCH

Administrator danych osobowych uwzględnia ryzyko naruszenia praw i wolności osób fizycznych, których dane dotyczą, wdrażając odpowiednie środki techniczne i organizacyjne celem zapewnienia stopnia bezpieczeństwa odpowiadającego temu ryzyku. Zarządzanie ryzykiem w Szkole Podstawowej nr 6 w Będzinie odbywa się zgodnie
z przyjętymi zasadami i z uwzględnieniem prawdopodobieństwa wystąpienia zagrożenia oraz jego skutków.

Administrator we współpracy z Inspektorem Ochrony Danych przeprowadza analizę ryzyka dla poszczególnych operacji przetwarzania danych w zakresie aktywów biorących udział w przetwarzaniu danych.
Celem zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń dokonuje się analizy ryzyka naruszenia praw i wolności osób, których dane dotyczą.
Administrator przeprowadza analizę ryzyka dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania.
W przypadku, gdy konieczne jest dokonanie oceny skutków dla ochrony danych osobowych podejmuje się następujące czynności:

- sporządzenie opisu planowanych operacji przetwarzania danych osobowych z określeniem celu przetwarzania dla każdej z nich (Rejestr Czynności Przetwarzania Danych);
- diagnoza zagrożeń związanych z wykorzystaniem aktywów stosowanych w procesie przetwarzania danych osobowych;
- ocena poziomu ryzyka, zgodnie z przyjętymi w Placówce zasadami;
- sporządzenie macierzy ze wskazaniem istotności ryzyka;
- przygotowanie raportu i wdrożenie planu naprawczego przewidującego środki techniczne, organizacyjne i informatyczne odpowiednie dla ryzyk, których stopień przekracza poziom średni.

9. SANKCJE KARNE

Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo, do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Niedopuszczalne albo nieuprawnione przetwarzanie dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

10. ZAŁĄCZNIKI

- Wykaz budynków i pomieszczeń stanowiących obszar przetwarzania danych osobowych – zgodnie z wykazem poprzedniej Polityki;
- Wykaz zbiorów danych osobowych – zgodnie z wykazem poprzedniej Polityki;
- Wzór rejestru czynności przetwarzania danych osobowych (załącznik nr 1);
- Wzór rejestru kategorii czynności przetwarzania danych osobowych dla podmiotu przetwarzającego (załącznik 2);
- Klauzula informacyjna (załącznik nr 3);
- Wzór umowy powierzenia przetwarzania danych osobowych (załącznik nr 4);
- Odwołanie upoważnienia do przetwarzania danych osobowych (załącznik nr 5);
- Upoważnienie do przetwarzania danych osobowych (załącznik nr 6);
- Ewidencja nadanych upoważnień (załącznik nr 7);
- Zgoda na przebywanie w obszarze przetwarzania danych osobowych (załącznik nr 8);
- Raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych (załącznik nr 9);
- Rejestr incydentów i naruszeń ochrony danych osobowych (załącznik nr 10);