POLITYKA OCHRONY DANYCH OSOBOWYCH

w Niepublicznej Szkole

Podstawowej Fundacji

Kannera

SPIS TREŚCI

1. WPROWADZENIE

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich przetwarzania w Niepublicznej Szkole Podstawowej Fundacji Kannera, dalej jako **Administrator** lub **Szkoła.**

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym.

Wszelkie zestawienia uzupełniające treść dokumentu zebrano w postaci załączników.

2. PODSTAWY PRAWNE

2.1. PRZEPISY PRAWA

Przepisy ochrony danych osobowych zawarte są w ustawie o ochronie danych osobowych oraz wydanych do niej aktach wykonawczych. Pełną listę aktów prawnych stanowią:

- 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) – RODO (Dz. Urz. UE 4.5.2016 PL L119);
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000).

2.2. DEFINICJE

W dokumencie przyjmuje się następującą terminologię:

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. ADO jest Niepubliczna Szkoła Podstawowa Fundacji Kannera, reprezentowana przez dyrektora.

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 (Dz. U. UE - 4.5.2016 L 119).

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. NAJWAŻNIEJSZE ZAGADNIENIA DOTYCZĄCE OCHRONY DANYCH OSOBOWYCH

3.1. PRZETWARZANIE DANYCH

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

2. PRZETWARZANIE ZWYKŁYCH DANYCH OSOBOWYCH

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.

3. PRZETWARZANIE SZCZGÓLNYCH KATEGORII DANYCH OSOBOWYCH

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.

3.2. UPOWAŻNIENIA

1. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. 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.
2. Przed wydaniem upoważnienia do przetwarzania danych osobowych, osoba mająca takie upoważnienie uzyskać ma obowiązek zapoznania się z aktualną Polityką Ochrony Danych Osobowych.
3. Upoważnienia nadaje się w zakresie czynności określonych w prowadzonym Rejestrze Czynności Przetwarzania Danych.

4. Upoważnienie wydane może być na czas określony zgodnie z trwaniem relacji na linii ADO – osoba upoważniona.

5. 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 upoważnienia.

6. Wzór upoważnienia do przetwarzania danych osobowych stanowi **załącznik nr 1** do niniejszej Polityki.

7. Prowadzona jest również ewidencja nadanych upoważnień, której wzór stanowi **załącznik nr 2.**

8. Za prowadzenie ewidencji oraz fizyczne wypisanie upoważnienia odpowiedzialny jest samodzielny referent ds. kadr i płac.

3.3. REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

1. REJESTR CZYNNOŚCI PRZETWARZANIA

Istotnym elementem Polityki Ochrony Danych, a także całego procesu zarzadzania danymi osobowymi przez Administratora Danych jest Rejestr Czynności Przetwarzania Danych Osobowych (RCPD)**.** 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.

2. BUDOWA RCPD

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

- 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

2. Rejestr prowadzony jest pisemnie, w formie elektronicznej przez osobę wyznaczona przez Administratora.

3. REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

1. 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.
2. Rejestr prowadzi się zgodnie z wytycznymi określonymi w art. 28 ust. 2 RODO.
3. Rejestr prowadzony jest pisemnie, w formie elektronicznej przez osobę wyznaczoną przez Administratora.

3.4. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. 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).

2. Przetwarzanie danych osobowych przez podmioty przetwarzające odbywa się na podstawie udokumentowanego polecenia Administratora w postaci umowy powierzenia przetwarzania danych osobowych zawartej z podmiotem przetwarzającym.
3. Wzór umowy powierzenia przetwarzania danych osobowych stanowi **załącznik nr 3**.

3.5. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Administrator danych osobowych zobowiązany jest do udzielania osobom, których dane dotyczą, informacji wskazanych w art. 13 i 14 RODO, a także odpowiadać na wnioski i żądania podmiotów danych w zakresie realizacji ich praw przewidzianych w art. 15-22 RODO.

2. Administrator przy kontakcie z podmiotem danych dokłada wszelkich starań, by komunikacja prowadzona z podmiotem danych była prowadzona w zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie, jasnym i prostym językiem.

3. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Dopuszcza się możliwość udzielenia informacji ustnie w sytuacji, w której osoba wnioskująca tego zażąda, ale tylko po zweryfikowaniu jej tożsamości.

4. W przypadku otrzymania wniosku lub żądania Administrator każdorazowo weryfikuje tożsamość osoby, która skierowała wniosek lub żądanie.

5. Administrator ewidencjonuje każde żądanie/wniosek podmiotu danych. Wzór rejestru realizacji żądań podmiotu danych stanowi **załącznik nr 6**.

6. Administrator udziela podmiotowi danych informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15-22 bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania.

7. Termin udzielenia informacji w razie potrzeby może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczby żądań. W omawianym przypadku Administrator w terminie miesiąca od otrzymania żądania informuje osobę, której dane dotyczą, o takim przedłużeniu oraz wskazuje przyczyny opóźnienia.

4. ZAGROŻENIA BEZPIECZEŃSTWA I POSTĘPOWANIE PRZY NARUSZENIACH OCHRONY DANYCH OSOBOWYCH

4.1. CHARAKTERYSTYKA MOŻLIWYCH ZAGROŻEŃ

- **Zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu.
- **Zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki przetwarzających dane, pozostawienie danych lub pomieszczeń bez nadzoru, błędy operatorów systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych lub naruszenia ich poufności.
- **Zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych. Zagrożenia te możemy podzielić na:

nieuprawniony dostęp z zewnątrz (włamanie), nieuprawniony dostęp do danych w wewnątrz (przez osoby nieuprawnione).

4.2. LISTA POTENCJALNYCH ZAGROŻEŃ BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Poniżej przedstawiono listy potencjalnych zagrożeń bezpieczeństwa danych z podziałem na zagrożenia miejsc przetwarzania oraz rodzajów danych, tj. zbiorów przetwarzanych tradycyjnie (papierowo) oraz z wykorzystaniem systemów informatycznych.

W każdym przypadku, w sytuacji stwierdzenia wystąpienia któregokolwiek z zagrożeń należy niezwłocznie powiadomić o tym fakcie samodzielnego referenda ds. kadr i płac.

- **Zagrożenia miejsc przetwarzania danych.**
  - Włamania od strony okien – wybite szyby, niedomknięte skrzydła.
  - Włamania od strony drzwi – zerwane plomby, uszkodzone klamki, źle działające zamki, niedomknięte drzwi, ślady po narzędziach.
  - Oddziaływanie czynników zewnętrznych – wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana.
  - Pozostawienie niezamkniętych drzwi lub okien – jeżeli w pomieszczeniu nie pozostają osoby uprawnione do przetwarzania danych.
  - Pozostawienie bez nadzoru osób nieuprawnionych do przebywania w pomieszczeniach.
- **Zagrożenia związane z przetwarzaniem danych papierowych.**
  - Pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy.
  - Pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze.
  - Pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe.
  - Przechowywanie dokumentów w miejscach do tego nieprzeznaczonych.

- Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.
- Przetwarzanie danych przez osoby nieuprawione.
- Nieuzasadnione sporządzanie kserokopii danych.

- **Zagrożenia związane z przetwarzaniem danych elektronicznych.**
  - Dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłanie poprzez Internet danych niezaszyfrowanych.
  - Dopuszczanie do nieuzasadnionego kopiowania dokumentów i utraty kontroli nad kopią.
  - Sporządzanie kopii danych w sytuacjach nieprzewidzianych procedurą.
  - Utrata kontroli nad kopią danych osobowych.
  - Podmiana lub zniszczenie nośników z danymi osobowymi.
  - Pozostawienie zapisanego hasła dostępu do bazy danych.
  - Samodzielne instalowanie jakiegokolwiek oprogramowania.
  - Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.
  - Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.
  - Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.
  - Niezabezpieczenie komputera zasilaczem awaryjnym podtrzymującym napięcie na wypadek braku zasilania.
  - Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych.
  - Ujawnianie sposobu działania aplikacji oraz jej zabezpieczeń osobom niepowołanym.
  - Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.

- Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.
- Pojawianie się komunikatów alarmowych.
- Awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich.
- Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.
- Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.
- Próba nieuzasadnionego przeglądania danych w ramach pomocy technicznej.
- Dopuszczanie, aby osoby inne niż ASI lub osoby przez ASI uprawnione, podłączały jakikolwiek urządzenia, demontowały elementy sieci lub dokonywały innych manipulacji.
- Ślady manipulacji przy układach sieci komputerowej lub komputerach.
- Obecność nowych urządzeń i kabli o nieznanym przeznaczeniu i pochodzeniu.
- Naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji

4.3. STOSOWANE ŚRODKI OCHRONY DANYCH OSOBOWYCH

1. ŚRODKI ORGANIZACYJNE

1. W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, Administrator danych wprowadza określone poniżej środki organizacyjne.

- Przetwarzanie danych osobowych u Administratora może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- Prowadzona jest **ewidencja osób upoważnionych** do przetwarzania danych.

- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne **upoważnienie**. Wzór upoważnienia stanowi **załącznik nr 1** do niniejszej dokumentacji.
- Każdy pracownik Administratora co najmniej raz na 2 lata powinien odbyć szkolenie z zakresu ochrony danych osobowych. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.
- Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
- Nie należy gromadzić w podręcznej dokumentacji danych osobowych.
- Dokumenty zawierające dane osobowe należy niszczyć w specjalistycznych niszczarkach.
- Każdorazowe zbieranie danych rodzi obowiązek informacyjny. Obowiązek należy realizować umieszczając odpowiednią treść informacyjną pod formularzem z danymi.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza siedzibę Administratora lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
- Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczać stosując wytyczne zawarte w Instrukcji zarządzania systemem informatycznym będącej częścią niniejszej dokumentacji.
- W celu zapewnienia danych przetwarzanych elektronicznie należy zapewnić logowanie do systemu operacyjnego (np. WINDOWS) oraz bezpośrednio do programów przetwarzających dane.

- Szczegółowe zasady postępowania ze zbiorami przetwarzanymi elektronicznie określa Instrukcja zarządzania systemem informatycznym będąca częścią niniejszej dokumentacji.

2. Dla celów obsługi i zabezpieczenia systemu informatycznego Administrator danych może powołać **Administratora systemu informatycznego** i wyznaczyć mu następujący zakres zadań:

- prowadzenie monitoringu przetwarzania danych,
- administrowanie systemem informatycznym,
- nadawanie uprawnień użytkownikom,
- stosowanie środków ochrony w ramach oprogramowania użytkowego, systemów operacyjnych, urządzeń teletransmisyjnych, programów antywirusowych oraz ochrony sprzętowej,
- kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych,
- kontrola systemu antywirusowego,
- kontrola awaryjnego zasilania komputerów,
- kontrola i wykonywanie kopii awaryjnych,
- konserwacja oraz uaktualnienia systemów informatycznych,
- informowanie na bieżąco ADO o przypadkach awarii programowych wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem, nie przestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystywania sprzętu komputerowego,
- przedstawianie Administratorowi danych, nie rzadziej niż raz na rok, kompleksowej analizy przetwarzania danych osobowych w systemem informatycznym oraz ewentualne potrzeby w zakresie zabezpieczeń.
- W przypadku kiedy ADO nie powołuje ASI wszystkie zapisy w dokumentacji, które odwołują się do ASI są rozumiane jako zapisy dot. ADO.

2. ŚRODKI TECHNICZNE

1. Potencjalne środki ochrony technicznej danych osobowych.

- **Ogólna ochrona budynku** – alarm antywłamaniowy, całodobowy dozór służb ochrony, gaśnice lub systemy p-poż.
- **Zabezpieczenia okien** – pomieszczenia zlokalizowane na parterze lub wyższych kondygnacjach można dodatkowo zabezpieczyć poprzez montaż krat, rolet lub szyb antywłamaniowych, zwłaszcza, jeśli istnieje do nich dostęp przez tarasy, dachy niższych budynków, drabiny p-poż, itp.
- **Zabezpieczenie drzwi** – w zależności od kategorii danych i zagrożeń można stosować drzwi tradycyjne zamykane na klucz lub p-pożarowe, zaś w miejscach szczególnie narażonych na zagrożenia (drzwi wejściowe, sekretariaty, księgowość, archiwa, itp.) **należy** stosować drzwi antywłamaniowe.
- **Zabezpieczenia zbiorów tradycyjnych (papierowych)** – w zależności od kategorii danych i zagrożeń do przechowywania danych można stosować szafy tradycyjne zamykane na klucz, szafy metalowe lub sejfy (dla danych szczególnie ważnych). Dane przeznaczone do zniszczenia **należy** niszczyć w specjalistycznych niszczarkach.
- **Zabezpieczenia zbiorów elektronicznych** – dane elektroniczne **należy** zabezpieczyć poprzez wyposażenie komputerów w zasilacze awaryjne podtrzymujące napięcie na wypadek braku zasilania oraz w systemy antywirusowe. Kopie danych **należy** gromadzić w szafach metalowych lub sejfach ognioodpornych.

2. Środki ochrony technicznej budynku stosowane u Administratora.

Administrator posiada następujący system zabezpieczeń:

- dostęp do kluczy mają upoważnione osoby obsługi,
- po zakończonym dniu pracy, drzwi zamykane są na klucz.

3. Każdy komputer przetwarzający dane osobowe zabezpieczono w zasilacz awaryjny podtrzymujący napięcie na wypadek braku zasilania oraz w system antywirusowy.

4. Dodatkowe, środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określono w **Instrukcji**

Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych będącej częścią niniejszej dokumentacji.

4.4 NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. RODZAJE NARUSZEŃ

1. Każde naruszenie bądź podejrzenie naruszenia zasad ochrony danych osobowych powinno być niezwłocznie zgłaszane dyrektorowi.

2. Za naruszenie lub próbę naruszenia zasad przetwarzania danych osobowych u Administratora 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.

2. METODYKA OCENY ZDARZENIA

Oceny wagi naruszenia dokonuje się na podstawie wytycznych Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), wg następującego schematu:

WN = KPD x PI + ON

Waga Naruszenia - **WN**

• kontekst Przetwarzania Danych - **KPD** – główny czynnik określający poziom krytyczności zestawu naruszonych danych, w określonym kontekście przetwarzania

• prawdopodobieństwo Identyfikacji - **PI** – czynnik korygujący KPD, który może obniżyć wynik.

Prawdopodobieństwo (łatwość) identyfikacji osoby na podstawie naruszonych danych dla osób, które uzyskały dostęp do nich.

• okoliczności Naruszenia - **ON** – czynnik, który odnosi się do okoliczności naruszenia, które wystąpiły lub nie w danym przypadku.

Kontekst Przetwarzania Danych

KPD = A + B

A – rodzaj i poziom wrażliwości danych	Dane podstawowe = 1
	Dane dotyczące zachowań osoby = 2
	Dane finansowe = 3
	Dane szczególne = 4
B – kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę	Szeroki zakres danych/wolumen danych (+)
	Charakter danych (+/-)
	Specyfika podmiotu danych lub administratora (+/-)
	Możliwe negatywne skutki dla podmiotu danych (+)
	Publiczna dostępność danych przed naruszeniem (-)
	Nieważność danych (-)

Prawdopodobieństwo identyfikacji - **PI**

Prawdo-podobieństwo identyfikacji	Znikome	= 0,25
	Ograniczone	= 0,5
	Wysokie	= 0,75
	Maksymalne	= 1

Okoliczności Naruszenia - **ON**

ON = NP + NI + ND + IDS

Naruszenie Poufności – Dane ujawnione	znanym odbiorcom danych (+0,25)
	nieznanej liczbie odbiorców danych (+0,5)
Naruszenie Integralności - Dane zmienione i	możliwe jest ich odzyskanie (+0,25)
	brak jest możliwości ich odzyskania (+0,5)
Naruszenie Dostępności - Niedostępność danych	czasowa (+0,25)
	pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5)

Intencjonalne Działanie Sprawcy (+0,5)

Ocena wagi naruszenia

Wynik	Waga naruszenia	Opis
WN<2	Niska	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności
2<=**WN**<3	Średnia	Osoby mogą napotkać niedogodności, które są możliwe do pokonania
3<=**WN**<4	Wysoka	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami
4<=**WN**	Bardzo wysoka	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje

3. REJESTRACJA NARUSZEŃ

1. 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.

2. Czynności te ujęte są w raporcie z naruszenia bezpieczeństwa zasad ochrony danych osobowych – **załącznik nr 4.**

3. W przypadku stwierdzenia wystąpienia naruszenia ochrony danych osobowych, prowadzi się 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.

4. 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 5.**

Protokoły ze zdarzenia oraz rejestr naruszeń sporządza i prowadzi samodzielny referent ds. kadr i płac.

4. ZGŁOSZENIE NARUSZENIA

1. 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.

2. 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.

5. POWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ

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

- dane Administratora Danych Osobowych
- dane IOD (osoba kontaktowa);
- datę 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.

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

5. ANALIZA RYZYKA I OCENA SKUTKÓW DLA OCHRONY DANYCH

1. ANALIZA RYZYKA

1. Administrator przeprowadza analizę ryzyka dla poszczególnych operacji przetwarzania danych w zakresie aktywów biorących udział w przetwarzaniu danych.

2. Celem zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń dokonuje się analizy ryzyka naruszenia praw i wolności osób, których dane dotyczą.

3. Administrator przeprowadza analizę ryzyka dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania.

4. Dla każdego istotnego zidentyfikowanego ryzyka właściciel ryzyka wskazuje optymalną reakcję. Przyjmuje się niżej wymienione reakcje na ryzyko:

- tolerowanie – będzie to miało miejsce w przypadkach, kiedy koszty skutecznego przeciwdziałania ryzyku mogą przekraczać jego potencjalne korzyści, z zdolności do skutecznego przeciwdziałania są ograniczone lub wykraczające poza decyzje i działania wewnętrzne;
- przeniesienie – dotyczyć to będzie kategorii ryzyk w odniesieniu do których nastąpi przeniesienie ich na inna instytucję, między innymi poprzez ubezpieczenie lub zlecenie usług na zewnątrz;
- wycofanie się – dotyczyć to będzie grypy ryzyk dla których mimo podejmowanych działań nie udało się zmniejszyć ich istotności do akceptowanego poziomu;
- przeciwdziałanie – dotyczyć to będzie kategorii ryzyk, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań prowadzących do ich likwidacji, lub znacznego ograniczenia.

5. Przy ocenie prawdopodobnych skutków wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie;

- 1 – oznacza skutek nieznaczny;
- 2 – oznacza skutek mały;
- 3 – oznacza skutek średni;
- 4 – oznacza skutek poważny;
- 5 – oznacza skutek katastrofalny.

6. Przy ocenie prawdopodobieństwa wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie:

- 1 – oznacza prawdopodobieństwo rzadkie (0-20 %);
- 2 – oznacza prawdopodobieństwo małe (21 - 40%);
- 3 – oznacza prawdopodobieństwo możliwe(41 - 60 %);
- 4 – oznacza prawdopodobieństwo prawdopodobne(61 - 80 %);
- 5 – oznacza prawdopodobieństwo prawie pewne (81 -100 %).

2. OCENA SKUTKÓW DLA OCHRONY DANYCH

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 u Administratora 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.

6. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

1. CHARAKTERYSTYKA SYSTEMU

1. Sieć informatyczną, w której przetwarzane są dane osobowe stanowią wszystkie pracujące u Administratora obecne i przyszłe serwery, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.
2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.
3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym w każdej jednostce komputerowej.

2. OGÓLNE ZASADY PRACY W SYSTEMIE INFORMATYCZNYM

1. Za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych, odpowiada

samodzielny referent ds. kadr i płac po podjęciu informacji od samodzielnego referenta ds. administracji.

2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone do eksploatacji licencjonowane oprogramowanie.
3. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
    a. mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu,
    b. mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej,
    c. mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
    d. urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,
    e. mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,
    f. mechanizmy zarządzania zmianami.
4. Użytkownikom zabrania się:
    a. udostępniania stanowisk roboczych osobom nieuprawnionym,
    b. wykorzystywania sieci komputerowej Administratora w celach innych niż związane z realizacją obowiązków służbowych,
    c. samowolnego instalowania i używania programów komputerowych,
    d. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
    e. umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej Administratora oraz sieci Internetowej osobom nieuprawnionym,
    f. używania komputera bez zainstalowanego oprogramowania antywirusowego.

3. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

1. Użytkowników systemów informatycznego tworzy oraz usuwa wyznaczona osoba na polecenie dyrektora .
2. Pracownicy otrzymują dostęp do poczty elektronicznej. Adres mailowy tworzy zewnętrzny podmiot świadczący usługi IT.
3. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
4. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
5. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

4. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Użytkownik posiadający upoważnienie do przetwarzania danych osobowych powinien posiadać hasła do systemu operacyjnego oraz osobne do baz danych osobowych i aplikacji.
3. Hasło do skrzynki mailowej składa się z co najmniej 12 znaków, zawiera co najmniej jedną małą i wielką literę, jedną cyfrę lub jeden znak specjalny.
4. Hasła do programów składają się z co najmniej 12 znaków, zawierają co najmniej jedną małą i wielką literę, jedną cyfrę lub jeden znak specjalny.

5. Hasło nie powinno zawierać żadnych informacji, które można skojarzyć z użytkownikiem komputera (imiona najbliższych, daty urodzenia, inicjały, itp.) i nie może być sekwencją kolejnych znaków klawiatury.
6. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do zgłoszenia tego faktu referentowi ds. administracji i do natychmiastowej zmiany hasła.
7. Hasła użytkowników generuje, w zależności od kontekstu, wskazana osoba i przekazuje bezpośrednio nowemu użytkownikowi.
8. Hasła do poczty elektronicznej generowane jest automatycznie.
9. Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do zmiany hasła na własne.
10. Hasło nie może być zapisywane i przechowywane.
11. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.
12. Komputery przenośne oraz inne mobilne nośniki danych osobowych powinny być zabezpieczone ochroną kryptograficzną – powinny być zaszyfrowane.

5. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy pracownik korzystający z systemu informatycznego przystępując do pracy powinien podać swoje dane dostępu do komputera i systemu, tj. identyfikator i hasło.
2. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.
3. Zakończenie pracy w systemie następuje poprzez prawidłowe, wymagane przez daną aplikację oraz system operacyjny, wykonanie czynności kończących. Niedopuszczalne jest zakończenie pracy poprzez wyłączenie napięcia zasilającego bez pełnej procedury zamknięcia.

4. Ekrany monitorów stanowisk komputerowych, na których odbywa się przetwarzanie danych osobowych powinny być w miarę możliwości tak umieszczone, aby uniemożliwić wgląd w dane osobom postronnym przebywającym w pomieszczeniu oraz powinny automatycznie się wyłączać poprzez stosowanie wygaszaczy ekranowych uruchamiających blokadę pracy na komputerze.
5. Osoba przetwarzająca dane osobowe w przypadku konieczności opuszczenia pomieszczenia, obowiązana jest prawidłowo, zgodnie z instrukcją obsługi systemu, zakończyć pracę w systemie.
6. Czas rozpoczynania i kończenia pracy w systemach sieciowych, w tym systemach przetwarzających dane osobowe, określają wewnętrzne zasady.

6. PROCEDURA TWORZENIA KOPII AWARYJNYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.
2. Ochronie poprzez wykonanie kopii podlegają programy i narzędzia programowe służące przetwarzaniu danych.
3. Kopia zapasowa wykonywana zgodnie z harmonogramem.

7. SPOSÓB ZABEZPIECZANIA SYSTEMU PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. Za ochronę antywirusową oraz zarządzaniem systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody odpowiedzialna jest osoba wyznaczona (informatyk).

2. System antywirusowy jest skonfigurowany w sposób zapewniający na bieżąco skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej i stron internetowych.
3. System antywirusowy musi mieć aktywną funkcję automatycznej aktualizacji wzorców wirusów.
4. W przypadkach zaistnienia sytuacji wskazującej na zainfekowanie systemu złośliwym oprogramowaniem użytkownik powinien niezwłocznie powiadomić o tym fakcie referenta ds. administracji.
5. W przypadku zainfekowania złośliwym oprogramowaniem i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, zewnętrzny podmiot świadczący usługi IT na zlecenie samodzielnego referenta ds. administracji r podejmuje działania zmierzające do usunięcia zagrożenia.

8. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. 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.
2. Instalacji, konserwacji oraz napraw sprzętu komputerowego dokonują osoby wskazane przez referenta ds. administracji.

3. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO lub posiadające umowy powierzenia przetwarzania danych w zakresie konserwacji i napraw.
4. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

7. SANKCJE KARNE

1. 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.

2. 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.

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

8. ZAŁĄCZNIKI

Załącznik nr 1. Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 2. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 3. Wzór umowy powierzenia przetwarzania danych osobowych.

Załącznik nr 4. Wzór raportu z naruszenia bezpieczeństwa zasad ochrony danych osobowych.

Załącznik nr 5. Wzór rejestru naruszeń bezpieczeństwa zasad ochrony danych osobowych.

Załącznik nr 6. Wzór rejestru realizacji żądań podmiotu danych.

ZAŁĄCZNIK NR 1 – WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

……., dn. ……

OBOWIĄZUJE:

od:……

do:……

UPOWAŻNIENIE nr _____

Na podstawie art. 29 rozporządzenia 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 119/50) – dalej RODO, ……. upoważnia Panią/Pana:

_____*(imię i nazwisko)*

_____ *(stanowisko)*

do przetwarzania, w ramach wykonywanych obowiązków służbowych, następujących czynności:

Zakres czynności	Identyfikator (login)

_____

(podpis przedstawiciela Administratora)

Stwierdzam własnoręcznym podpisem, że znana mi jest treść dokumentacji ochrony danych osobowych w Niepublicznej Szkole Podstawowej Fundacji Kannera.

Jednocześnie zobowiązuję się nie ujawniać danych, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy, a w szczególności nie będę:

a) ujawniać danych zawartych w eksploatowanych w systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
b) ujawniać szczegółów technologicznych używanych w systemów oraz oprogramowania,
c) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą dokumentacją.

_____

(podpis osoby upoważnionej)

ZAŁĄCZNIK NR 2 – WZÓR EWIDENCJI NADANYCH UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

w Niepublicznej Szkole Podstawowej Fundacji Kannera

Nr upoważnienia	Imię i nazwisko osoby upoważnionej	Data		Zakres upoważnienia	Identyfikator (login)
		nadania upoważnienia	ustania upoważnienia		

ZAŁĄCZNIK NR 3 – WZÓR UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

(zwana dalej „Umową")

_____ *(dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Podmiotem przetwarzającym"**

reprezentowana przez:

_____

oraz

_____ *(dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Administratorem danych" lub „Administratorem"**

reprezentowana przez:

_____

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający przetwarza powierzone dane osobowe tylko na wyraźne polecenie Administratora danych.
3. Przetwarzanie powierzonych danych osobowych przez Podmiot przetwarzający będzie polegało na ……..

4. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
5. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§ 2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane osobowe ……. *(należy podać kategorię osób, których dane dotyczą*) *w postaci ……*
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu …….. *(należy podać cel przetwarzania danych przez podmiot przetwarzający*) przez okres ……..*(należy wskazać okres czasu bądź kryterium jego ustalenia)*

§ 3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu ….. *(można wskazać np. w ciągu 24 h).*

§ 4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum …….. *(należy wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli*) jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni *(administrator termin może określić dowolnie).*
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§ 7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony/określony do ……..
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem …… okresu wypowiedzenia.

§ 8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§ 9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§ 10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych *(lub Podmiotu przetwarzającego w zależności od postanowień stron*).

_____ _____

Administrator danych Podmiot przetwarzający

ZAŁĄCZNIK NR 4 – WZÓR RAPORTU NARUSZEŃ BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w Niepublicznej Szkole Podstawowej Fundacji Kannera

Data zdarzenia: _____ Godzina: _____

Osoba powiadamiająca o zaistniałym zdarzeniu:

_____

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

Lokalizacja zdarzenia:

_____

(np. nr pokoju, nazwa pomieszczenia)

Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

_____
_____
_____
_____
_____
_____
_____

Możliwe konsekwencje naruszenia ochrony danych osobowych (w tym dla osób, których dane dotyczą):

_____
_____
_____
_____
_____

_____

Przyczyny wystąpienia zdarzenia:

_____

_____

_____

_____

_____

Postępowanie wyjaśniające:

_____

_____

_____

_____

_____

Podjęte działania naprawcze:

_____

_____

_____

_____

_____

_____

_____

_____

_____

(podpis przedstawiciela Administratora)

ZAŁĄCZNIK NR 5 – WZÓR REJESTRU NARUSZEŃ BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

w Niepublicznej Szkole Podstawowej Fundacji Kannera

Lp.	Data naruszenia	Godzina naruszenia	Kategorie osób, których danych dotyczy naruszenie	Ilość osób	Ilość naruszonych wpisów danych	Nr raportu	Data zawiadomienia organu	Informacja o zawiadomieniu osób, których dane dotyczą/powód niezawiadomienia
1								
2								
3								
4								
5								
6								
7								
8								

ZAŁĄCZNIK NR 6 – WZÓR REJESTRU REALIZACJI ŻĄDAŃ PODMIOTU DANYCH

Żądanie podmiotu danych nr:

I. Żądanie

1. Data zgłoszenia żądania:

……..

2. Forma zgłoszenia żądania (kanał komunikacji):

……..

3. Zgłaszający żądanie:

……..

4. Treść żądania:

……..

II. Obsługa żądania

1. Pracownik obsługujący żądanie:

……..

2. Czy dane zgłaszającego żądanie są przetwarzane przez administratora danych:

……..

3. Czy dane zgłaszającego żądanie zostały powierzone (komu, kiedy):

……..

4. Podjęte czynności:

a) Czynność I

- Osoba podejmująca czynność:

……..

- Opis czynności:

……..

- Data dokonania czynności:

……..

b) Czynność II

- Osoba podejmująca czynność:

……..

- Opis czynności:

……..

- Data dokonania czynności:

……..