Placówka Opiekuńczo-Wychowawcza Nr 1
44-335 Jastrzębie-Zdrój
ul. Opolska 7/1-2
NIP 633 223 93 90
tel. 32 47 67 406

ZARZĄDZENIE NR 0211.23.2019

Dyrektora Placówek Opiekuńczo – Wychowawczych Nr 1, 2, 3
w Jastrzębiu – Zdroju

z dnia 13 MARCA 2019 r.

w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych
w Placówkach Opiekuńczo – Wychowawczych Nr 1, 2, 3

z a r z ą d z a m

§ 1

Wprowadzam Politykę danych osobowych w Placówkach Opiekuńczo – Wychowawczych Nr 1, 2, 3

§ 2

Zarządzenie wchodzi w życie z dniem podjęcia z mocą obowiązująca od 2 stycznia 2019 r.

DYREKTOR
Placówek Opiekuńczo-Wychowawczych
Nr 1,2,3
mgr Izabela Grzybek

POLITYKA BEZPIECZEŃSTWA

DANYCH OSOBOWYCH

W PLACÓWKACH OPIEKUŃCZO -WYCHOWAWCZYCH
NR 1, NR 2 i NR 3 w JASTRZĘBIU-ZDROJU

Data i miejsce sporządzenia dokumentu:	Jastrzębie-Zdrój 02/01/2019
Ilość stron:	19
Zatwierdził:	DYREKTOR Placówek Opiekuńczo-Wychowawczych Nr 1,2,3 mgr Izabela Grzybek

1. Wstęp

Administratorem Danych, który wdraża Politykę Bezpieczeństwa jest Dyrektor Placówek Opiekuńczo - Wychowawczych nr 1, nr 2 i nr 3 w Jastrzębiu-Zdroju (44-335). Niniejsza Polityka jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w celu spełnienia wymagań Rozporządzenia Parlamentu Europejskiego I Rady (Ue) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 DZ.U.2018 poz. 1000. Dokument niniejszy stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z ogólnym rozporządzeniem o ochronie danych , a także usprawnienie i usystematyzowanie organizacji pracy w zakresie zapewnienia bezpieczeństwa danych osobowych przetwarzanych przez Administratora danych.

2. Definicje.

W Polityce przyjmuje się następującą terminologię:

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W ramach niniejszego dokumentu jest to **Dyrektor Placówek Opiekuńczo-Wychowawczych nr 1, nr 2 i nr 3 w Jastrzębiu Zdroju.**

RODO – ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO 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) 95/46 z 27 kwietnia 2016 r.

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną przez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden oraz więcej czynników specyficznych określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej o których mowa w art. 4 pkt 1 RODO.

Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie o których mowa w art. 4 pkt 2 RODO.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Anonimizacja - zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych. Jest to proces nieodwracalny.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. przez zastępowanie imienia i nazwiska liczbami lub innymi pseudonimami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym zapewniającym brak dostępu dla osób, które nie mają uprawnień nadanych przez administratora.

Zgoda osoby, której dane dotyczą - oznacza w pełni świadome i dobrowolne oświadczenie lub wyraźne działanie potwierdzające wyrażenie zgody na przetwarzanie danych osobowych przez osobę, której dane dotyczą, przy czym to Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo (wykaz rodzajów operacji przetwarzania wymagających oceny skutków opublikowany w Monitorze Polskim), lub w przypadku kiedy ryzyko naruszenia praw i wolności będzie wysokie.

Podmiot danych - osoba fizyczna, której dane dotyczą.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (procesor) - osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu Administratora.

Inspektor Ochrony Danych (IOD) - osoba wyznaczona przez Administratora w celu informowania i doradzania Administratorowi w zakresie obowiązującego prawa o ochronie danych oraz w celu monitorowania przestrzegania przepisów o ochronie danych oraz działająca jako punkt kontaktowy dla podmiotów danych, a także organu nadzorczego.

Szczególne kategorie danych osobowych oznaczają informacje na temat pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, stanu zdrowia, kodu genetycznego, nałogów lub życia seksualnego, skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Profilowanie – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Organ nadzorczy – Urząd Ochrony Danych Osobowych.

3. Dane osobowe.

1) Administrator przetwarza dane osobowe gromadzone w zbiorach danych.
2) **Dane osobowe domyślnie przetwarzane są na obszarze obejmującym pomieszczenia biurowe oraz pokoje wychowawców, psychologów, pedagogów, gabinety terapeutyczne zlokalizowane w Jastrzębiu-Zdroju w następujących obiektach:**

   a) Placówka Opiekuńczo- Wychowawcza nr 1 w Jastrzębiu-Zdroju, ul.Opolska 7/1-2,

   b) Placówka Opiekuńczo – Wychowawcza nr 2 w Jastrzębiu-Zdroju, ul. Opolska 7/3

   c) Placówka Opiekuńczo – Wychowawcza nr 3 w Jastrzębiu-Zdroju, ul. Turystyczna 23.

   Dodatkowy obszar, w którym przetwarzane są dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym w zdaniu poprzedzającym.

4. Upoważnienia.

1. Administrator upoważnia na piśmie wszystkie osoby, które w zakresie swoich czynności służbowych oraz realizowanych na polecenie administratora zadań mają dostęp do danych osobowych.
2. Osoby upoważnione oraz wszystkie inne osoby, którym udostępnia się dane osobowe zobowiązane są do przetwarzania danych osobowych zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych regulaminów lub procedur wewnętrznych związanych z przetwarzaniem danych osobowych.
3. Przy zatrudnianiu Pracowników oraz w toku zatrudnienia Administrator zapewnia, że:
   1) Pracownicy przed przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad przetwarzania i ochrony danych osobowych;
   2) Każdy z pracowników zostaje upoważniony na piśmie do przetwarzania danych osobowych w niezbędnym zakresie, zgodnie z wzorem stanowiącym **Załączniki nr 1** do Polityki;
4. Administrator odpowiada za nadawanie oraz odbieranie upoważnień do przetwarzania danych osobowych.
5. Każda osoba upoważniona może przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.
6. Upoważnienia nadawane są pracownikom, zleceniobiorcom, stażystom oraz innym osobom, które w ramach wykonywania czynności służbowych na rzecz Administratora mają dostęp do danych osobowych .
7. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do udziału w komisji zakładowej, do przeprowadzania audytu, wykonywania czynności służbowych przypisanych do stanowiska pracy.
8. Administrator prowadzi Ewidencję nadanych upoważnień według wzoru stanowiącego **załącznik nr 2** do Polityki.
9. Osoba, która przetwarza dane osobowe w systemie informatycznym uzyskuje dostęp do tego systemu poprzez nadanie loginu, jako indywidualnego identyfikatora służącego rozliczalności tego dostępu oraz hasło zabezpieczające.
10. Hasło dostępu należy bezwzględnie chronić i utrzymywać w tajemnicy.
11. Uprawnienie dostępu do systemu informatycznego może uzyskać wyłącznie osoba upoważniona przez administratora do przetwarzania danych osobowych.

12. Loginy podlegają wpisaniu do ewidencji nadanych upoważnień.
13. W Ewidencji nadanych upoważnień zamieszcza się następujące informacje: imię i nazwisko osoby upoważnionej, zajmowane stanowisko, loginy do systemów informatycznych, polecenie upoważnienia, datę nadania oraz ustania upoważnienia .
14. Upoważnienia do przetwarzania danych osobowych, nadane przed dniem wejścia w życie RODO , tj. do dnia 24 maja 2018 roku zachowują swoją ważność.
15. W związku z przejęciem pracowników na podstawie art. 23(1) Kodeksu Pracy przez Dyrektora Placówki Opiekuńczo Wychowawczej nr 1,2,3 w Jastrzębiu-Zdroju, została zachowana i jest kontynuowana Ewidencja nadanych upoważnień założona i prowadzona do dnia 31 grudnia 2018 roku przez Dyrektora zlikwidowanego Zespołu Ognisk Wychowawczych w Jastrzębiu-Zdroju. Ewidencja oraz upoważnienia zostały zachowane oraz są kontynuowane na podstawie niniejszej Polityki w celu zachowania ciągłości oraz rozliczalności.
16. W związku z przejęciem systemów informatycznych swoją ważność zachowują również loginy do systemów nadane przez Dyrektora zlikwidowanego Zespołu Ognisk Wychowawczych w Jastrzębiu-Zdroju.

5. Rejestr czynności przetwarzania.

1. Za pośrednictwem rejestru Administrator dokumentuje czynności przetwarzania danych osobowych oraz inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Poprzez wskazanie w rejestrze ogólnych środków ochrony danych osobowych objętych wyodrębnioną czynnością przetwarzania, Administrator dąży również do wykazania zgodności przetwarzania danych osobowych z wymogami prawa.
2. Prowadzenie **rejestru czynności przetwarzania** danych ma na celu zapewnienie zgodności z zasadami i warunkami przetwarzania danych osobowych. Dzięki danym zebranym w tym rejestrze administrator może ocenić, w jakim zakresie dotyczą go inne obowiązki wynikające z RODO np. obowiązek przeprowadzenia oceny skutków przetwarzania dla ochrony danych.
3. Rejestr pozwala zatem na stałą weryfikację działalności w zakresie przetwarzania danych osobowych oraz poddawanie ocenie każdego nowo wprowadzanego lub modyfikowanego procesu już na jego najwcześniejszym etapie.
4. W przypadku podjęcia się przez Administratora zadań procesora i przetwarzania danych

osobowych powierzonych przez innych administratorów, Administrator prowadzi dodatkowo **rejestr wszystkich kategorii czynności przetwarzania.**

6. Analiza ryzyka.

1. Administrator musi samodzielnie analizować ryzyko, uwzględniając wiele specyficznych dla niego czynników, takich jak: wielkość, struktura organizacyjna, możliwości techniczne, zakres i rodzaj danych, cel przetwarzania danych.
2. Szacowanie ryzyka to proces ciągły, który powinien być przeprowadzany przy użyciu konkretnej metody, zapewniającej jednocześnie stosowanie jednolitych definicji i pojęć.
3. Administrator danych przeprowadza analizę ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
4. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie czynności przetwarzania, które należy zabezpieczyć.
5. Poprzez określenie prawdopodobieństwa oraz skutków wystąpienia danego (niepożądanego) zdarzenia Administrator określa wysokość ryzyka wystąpienia incydentu.
6. Po przeprowadzeniu analizy ryzyka Administrator podejmuje określone działania skierowane na obniżenie wpływu ryzyka na funkcjonowanie danego podmiotu i dokonuje wyboru odpowiednich środków przeciwdziałania i minimalizacji ryzyka.
7. Oceniając prawdopodobieństwo wystąpienia danego zdarzenia należy wziąć pod uwagę istniejące mechanizmy kontrolne, ich skuteczność oraz poziom zaawansowania.
8. **Identyfikując prawdopodobieństwo wystąpienia zagrożenia Administrator kieruje się doświadczeniem oraz wiedzą na temat incydentów, które wystąpiły w przeszłości, jak również analizuje możliwość wystąpienia danego zagrożenia na podstawie informacji uzyskanych podczas inwentaryzacji czynności przetwarzania oraz osób, które mają dostęp do przetwarzania danych osobowych**.
9. Poziom istotności ryzyka jest iloczynem skali prawdopodobieństwa jego wystąpienia i wartości oszacowanych potencjalnych skutków.

$$R = P \times S$$

gdzie:

R – poziom istotności ryzyka

P – Prawdopodobieństwo wystąpienia zdarzenia

S – Skala oddziaływania w przypadku wystąpienia zdarzenia (Skutek).

10. 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 wysoki.

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

1 – oznacza prawdopodobieństwo bardzo małe (0-20 %),

2 – oznacza prawdopodobieństwo małe (21 - 40%),

3 – oznacza prawdopodobieństwo średnie (41 - 60 %),

4 – oznacza prawdopodobieństwo duże (61 - 80 %),

5 – oznacza prawdopodobieństwo wysokie (81 -100 %).

12. W celu dokonania oceny ryzyka wykorzystuje się mapę istotności ryzyka, która stanowi macierz prawdopodobieństwo-skutek.

Prawdopodobieństwo						
Wysokie	5	10	15	20	25	
Duże	4	8	12	16	20	
Średnie	3	6	9	12	15	
Małe	2	4	6	8	10	
B.małe	1	2	3	4	5	
	Nieznaczny	Mały	Średni	Poważny	Wysoki	Skutek

13. Mapa ryzyka definiuje ryzyka na :
    1) niskie o wartości 4 i mniejszej;
    2) średnie o wartości powyżej 4 i mniejszej niż 15;
    3) wysokie – o wartości powyżej 15.

14. Dla każdego zidentyfikowanego i poddanego analizie ryzyka właściciel ryzyka wskazuje optymalną reakcję, do których zaliczamy:

    1) **Tolerowanie** – w przypadkach, kiedy możliwość przeciwdziałania jest ograniczona lub koszty skutecznego przeciwdziałania ryzyku mogą przekroczyć przewidziane korzyści, a także gdy poziom ryzyka jest akceptowalny;

    2) **Przeniesienie** – dotyczyć to będzie kategorii ryzyk w odniesieniu do których nastąpi przeniesienie ich na inny podmiot np. poprzez ubezpieczenie lub zlecenie usług na zewnątrz;

    3) **Działanie** – dotyczyć to będzie kategorii ryzyk, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań zaradczych w celu zmniejszenia ryzyka do poziomu akceptowalnego lub jego likwidacji;

    4) **Wycofanie** – zaniechanie działań powodujących zbyt duże ryzyko.

15. Wzór arkusza zarządzania ryzykiem stanowi **załącznik nr 10** do Polityki.

16. Metoda oceny ryzyka przedstawiona powyżej nie stanowi jedynej, dopuszczonej przez Administratora metody szacowania tego ryzyka.

17. Ocena ryzyka dokonywana jako wykaz działań niosących ryzyko dla wolności i praw osób, których dotyczą, przeprowadzona zgodnie z wytycznymi grupy roboczej 29 - wp 248/2017, może mieć również zastosowanie, jeżeli w ocenie Administratora metoda ta pozwoli na ustalenie, czy dane ryzyko jest akceptowalne, czy nie akceptowalne.

18. Wzór oceny ryzyka wraz z oceną skutków stanowi **załącznik nr 11** do Polityki.

7. Zasady ochrony danych.

1. Administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną,

przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:

   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");

   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu");

   3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");

   4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");

   5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania");

   6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

3. Przy zapewnieniu przetwarzania danych osobowych zgodnie z zasadami wskazanymi wyżej Administrator opiera przetwarzanie na następujących podstawach:

   1) Legalność – Administrator dba o ochronę prywatności i przetwarza dane osobowe zgodnie z wymogami prawa;

   2) Bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych osobowych podejmując stale działania w tym zakresie;

   3) Prawa Jednostki – Administrator umożliwia osobom, których dane osobowe przetwarza, wykonywanie swoich praw i prawa te realizuje;

   4) Rozliczalność – Administrator zapewnia należyte udokumentowanie sposobu spełniania obowiązków w zakresie ochrony danych osobowych.

8. Bezpieczeństwo danych osobowych.

Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

1) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
2) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
3) dostosowuje środki ochrony danych do ustalonego ryzyka;
4) posiada system zarządzania bezpieczeństwem informacji;
5) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami;
6) dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających;
7) wprowadza regulaminy i instrukcje postępowania z danymi osobowymi.

9. Zadania oraz status Inspektora Ochrony Danych.

1. Do zadań Inspektora ochrony danych należy w szczególności:
   1) informowanie Dyrektora oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach wynikających z rozporządzenia RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach;
   2) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
   4) współpraca z organem nadzorczym, tj. Urzędem Ochrony Danych Osobowych;
   5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
2. Administrator publikuje na swojej stronie internetowej dane Inspektora Ochrony Danych, tj. imię i nazwisko oraz adres e-mail do kontaktu.

3. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
4. Administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
5. Administrator wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania.
6. Administrator zapewnia, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania swoich zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora.
7. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.
8. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
9. Jeżeli Inspektor ochrony danych miałby wykonywać inne zadania i obowiązki, niż wymienione w ust. 1 to Administrator zapewnia, by te zadania i obowiązki nie powodowały konfliktu interesów.
10. Wzór wyznaczenia określa **załącznik nr 7** do Polityki.

10. Postępowanie z incydentami oraz naruszeniami ochrony danych osobowych

Postępowanie Administratora danych osobowych lub osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia zagrożenia:

1) ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków,
2) w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,
3) w razie konieczności zainicjowanie działań dyscyplinarnych,
4) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,

5) udokumentowanie prowadzonego postępowania w rejestrze incydentów i naruszeń bezpieczeństwa danych osobowych zgodnie ze wzorem stanowiącym **załącznik nr 6** do niniejszej Polityki.

Administrator opracowuje szczegółową instrukcję postępowania na wypadek wystąpienia zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych oraz w przypadku naruszenia.

11. Szkolenia oraz oświadczenia o poufności

1. Osoby zatrudnione w obszarze przetwarzania przed dopuszczeniem do pracy z danymi osobowymi powinny być zapoznane przez Administratora z niniejszą Polityką bezpieczeństwa danych osobowych oraz zobowiązane do zachowania w tajemnicy przetwarzanych przez siebie danych osobowych w trakcie zatrudnienia jak i po jego ustaniu.
2. Oświadczenie pobiera się niezwłocznie po nadaniu upoważnienia do przetwarzania danych.
3. Osoby zatrudnione poza obszarem przetwarzania (np. sprzątaczki,kucharki) podpisują oświadczenie o poufności według wzoru stanowiącego **załącznik nr 3** do niniejszej Polityki ochrony danych osobowych.
4. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych przez Inspektora Ochrony Danych, wskazane jest udokumentowanie odbycia tego szkolenia.
5. Wewnętrzne szkolenie przypominające zostaje zakończone podpisaniem przez pracownika listy uczestników szkolenia, którą stanowi **załącznik nr 5** do Polityki. Kartę ze szkolenia wstępnego z zakresu ochrony danych osobowych stanowi **załącznik nr 4** do Polityki. Karty trzymane są w dokumentacji związanej z ochroną danych osobowych.

12. Audyty

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. Audyt przeprowadza Inspektor Ochrony Danych wraz z pracownikiem wyznaczonym przez Administratora.
3. Wzór protokółu z kontroli przetwarzania i stanu zabezpieczenia danych osobowych stanowi **załącznik nr 12** do Polityki.

13. Wykaz podstawowych zabezpieczeń stosowanych przez Administratora danych:

a. Środki organizacyjne:

1. Opracowano i wdrożono Politykę bezpieczeństwa danych osobowych.
2. Do przetwarzania danych dopuszczono wyłącznie osoby posiadające upoważnienia nadane przez Administratora Danych.
3. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
4. Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych.
5. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy.
6. Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
7. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
8. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
9. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
10. Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami (procesorami) przetwarzającymi dane osobowe – Administrator prowadzi wykaz umów powierzenia według wzoru stanowiącego **załącznik nr 8** do Polityki.
11. Administrator udostępnia dane osobowe na podstawie przepisów prawa lub za zgodą podmiotu danych.
12. W podmiocie prowadzi się politykę czystego biurka i ekranu.
13. Wdrożono procedurę (instrukcję) otwierania i zamykania budynków oraz pomieszczeń biurowych, z którą zapoznaje się odpowiedzialnych za tę czynność pracowników.

b. Środki ochrony fizycznej danych

1. Dane osobowe przechowywane są w pomieszczeniach zamykanych na klucz.
2. Jeżeli zbiór danych osobowych przechowywany jest w pomieszczeniu na parterze, to okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
3. Dane osobowe w formie papierowej są przechowywane w zamkniętych niemetalowych lub metalowych szafach.
4. Po zakończeniu pracy, przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w zamykanych szafach bądź biurkach.
5. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie.
6. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
7. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

c. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. Dostęp do internetu oraz sieci lokalnej zabezpieczony jest hasłem.
2. Zastosowano urządzenia typu UPS chroniący system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
3. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
5. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
6. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
7. Użyto system Firewall do ochrony dostępu do sieci komputerowej.

d. Środki ochrony w ramach narzędzi programowych i baz danych

1. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zastosowano kryptograficzne środki ochrony danych osobowych.
3. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
4. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

14. Prawa osób, których dane dotyczą.

1. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności, takich jak zgłoszenie sprzeciwu lub ograniczenie przetwarzania.

2. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane osobowe przetwarza.

3. Administrator pozostawia do wglądu w siedzibie klauzule informacyjną dotyczącą przetwarzania danych osobowych oraz praw podmiotów danych. Wzór klauzuli określa **załącznik nr 9** do niniejszej polityki.

4. W celu realizacji praw osoby, której dane osobowe dotyczą Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

5. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób, informując osobę, której dane dotyczą o:
   1) przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby;
   2) przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej;

3) planowanej zmianie celu przetwarzania danych;

4) przed uchyleniem ograniczenia przetwarzania;

5) sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba, że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe);

6) prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

6. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

7. Niezależnie od postanowień ust. 5 wyżej, Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe poprzez wywieszenie informacji o objęciu obszaru monitoringiem wizyjnym.

8. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

9. Administrator wydaje osobie, której dane osobowe dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

10. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której dane osobowe dotyczą. Administrator ma prawo odmówić sprostowania danych chyba, że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga.

11. Administrator uzupełnia i aktualizuje dane na żądanie osoby, której dane osobowe dotyczą. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby, co do uzupełnianych danych chyba, że będzie to niewystarczające w świetle przyjętych przez Administratora procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

12. Z uwzględnieniem ust. 13 niżej, na żądanie osoby, Administrator usuwa dane, gdy:

1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
4) dane były przetwarzane niezgodnie z prawem,
5) konieczność usunięcia wynika z obowiązku prawnego,
6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

13. Administrator przy usuwaniu danych osobowych uwzględnia, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

14. Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

1) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

3) Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

4) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

15. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą chyba, że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

16. Procedura (instrukcja) obsługi żądań podmiotów danych jest dokumentem, z którym Administrator zapoznaje pracowników odpowiedzialnych za tę czynność.

15. Postanowienia końcowe.

1. Polityka jest przechowywana i udostępniana w wersji papierowej w siedzibie Administratora.
2. Administrator w uzupełnieniu do niniejszej Polityki bezpieczeństwa danych osobowych , w celu uszczegółowienia niektórych procedur w niej zawartych, opracowuje i udostępnia do zapoznania się przez pracowników wyznaczonych do realizowania tych procedur, instrukcje określające szczegółowe zasady postępowania.
3. Wdrożenie instrukcji nie wymaga wprowadzenia zarządzeniem dyrektora jednostki.
4. Polityka niniejsza wchodzi w życie z mocą obowiązującą od 1 stycznia 2019 roku.

5. **Załączniki do Polityki:**

Nr załącznika	Opis załącznika
Załącznik nr 1	Upoważnienie do przetwarzania danych
Załącznik nr 2	Wzór ewidencji nadanych upoważnień
Załącznik nr 3	Klauzula poufności dla pracowników bez nadanego upoważnienia
Załącznik nr 4	Karta szkolenia wstępnego z zakresu ochrony danych osobowych
Załącznik nr 5	Lista uczestników szkolenia przypominającego
Załącznik nr 6	Wzór rejestru incydentów i naruszeń bezpieczeństwa danych osobowych
Załącznik nr 7	Wzór wyznaczenia IOD
Załącznik nr 8	Wykaz umów powierzenia
Załącznik nr 9	Wzór klauzuli informacyjnej
Załącznik nr 10	Wzór arkusza zarządzania ryzykiem
Załącznik nr 11	Wzór oceny ryzyka wraz z oceną skutków
Załącznik nr 12	Protokół z kontroli

.....
/pieczęć administratora danych /

Upoważnienie do przetwarzania danych osobowych - pracownik

Na podstawie ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (RODO) niniejszym upoważniam Panią / Pana :

imię i nazwisko: .....

zatrudnioną/ ego na stanowisku : .....

do przetwarzania od dnia ..... r. danych osobowych wyłącznie w zakresie wykonywania obowiązków służbowych na stanowisku pracy oraz poleceń przełożonego

Upoważnienie jest ważne do: dnia ustania stosunku pracy / ..... (*)

DOSTĘPY (LOGINY) DO SYSTEMÓW INFORMATYCZNYCH – jeżeli zostały nadane:

Program: ..... Login: ..... od ..... do .....

Program: ..... Login: ..... od ..... do .....

Program: ..... Login: ..... od ..... do .....

.....
/ Administrator Danych Osobowych/

Ja niżej podpisana/y oświadczam że :

1) przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/ em zaznajomiona/ y z przepisami dotyczącymi ochrony danych osobowych ;

2) zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w Regulaminie ochrony danych osobowych obowiązującym u Administratora oraz zobowiązuje się do ich przestrzegania.

Ponadto zobowiązuje się zachować w tajemnicy dane osobowe, które będę przetwarzał/a oraz znane mi sposoby zabezpieczenia danych osobowych przez cały okres zatrudnienia u Administratora , jak również po ustaniu zatrudnienia .

Przyjmuję do wiadomości , iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za naruszenie przepisów o ochronie danych osobowych .

.....
/osoba upoważniona do przetwarzania danych /

(*) jeżeli upoważnienie ustaje w innym terminie należy wskazać datę ustania upoważnienia

Załącznik nr 1 do Polityki

.....

(pieczęć Administratora Danych)

Upoważnienie do przetwarzania danych osobowych - zlecenie

Na podstawie art. 32 ust 4 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, zwane dalej RODO, upoważniam

Panią/Pana:.....

wykonującą/ego umowę zlecenie obejmującą czynności.....
do przetwarzania danych osobowych w związku z wykonywaniem czynności objętych zleceniem .

Upoważnienie udzielane jest na czas trwania umowy zlecenia.

.....
(podpis Administratora)

Ja niżej podpisana/y oświadczam że :

1) przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/ em zaznajomiona/ y z przepisami dotyczącymi ochrony danych osobowych ;
2) zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w dokumentacji przetwarzania danych osobowych obowiązującej u Administratora Danych Osobowych oraz zobowiązuje się do ich przestrzegania.

Ponadto zobowiązuje się zachować w tajemnicy dane osobowe, które będę przetwarzał/a oraz znane mi sposoby zabezpieczenia danych osobowych przez cały okres zatrudnienia u Administratora Danych Osobowych, jak również po ustaniu zatrudnienia .

Przyjmuję do wiadomości , iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za naruszenie przepisów o ochronie danych osobowych .

.....
/osoba upoważniona do przetwarzania danych /

załącznik nr 2

EWIDENCJA NADANYCH UPOWAŻNIEŃ

L.p	Imię i Nazwisko, zajmowane stanowisko /data zmiany danych/	Identyfikator w systemie informatycznym*	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania upoważnienia	Data ustania upoważnienia
1					
	Zmiana danych**				
2					
	Zmiana danych**				
3					
	Zmiana danych**				
4					
	Zmiana danych**				

.....
(imię i nazwisko)

.....
(miejscowość, data)

.....
(zajmowane stanowisko)

OŚWIADCZENIE O POUFNOŚCI

dla osób nie mających nadanego upoważnienia do przetwarzania danych osobowych, lecz wykonujących czynności w fizycznym obszarze przetwarzania

Oświadczam, iż zobowiązuję się do:

- zachowania w tajemnicy **danych osobowych,** do których mam lub będę miał/a dostęp w trakcie wykonywania czynności służbowych w fizycznym obszarze przetwarzania, a których administratorem/procesorem jest Pracodawca, w trakcie zatrudnienia oraz po ustaniu stosunku pracy,

- zgłaszania wszelkich zauważonych incydentów naruszenia zasad ochrony danych osobowych bezpośredniemu przełożonemu.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższym zobowiązaniem, może być uznane za naruszenie przepisów o ochronie danych osobowych.

.....
podpis

.....
(pieczęć Administratora danych)

Załącznik nr 4 do Polityki

Karta szkolenia wstępnego z zakresu ochrony danych osobowych

Imię i nazwisko osoby szkolonej:	
Stanowisko:	**Data instruktażu:**
Nazwa administratora danych:	

Zasady przetwarzania danych przez osoby posiadających upoważnienia do przetwarzania danych osobowych:

1) Dostęp do danych osobowych mogą mieć wyłącznie osoby posiadające upoważnienie do przetwarzania danych.
2) Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu danych.
3) Dane muszą być chronione przed dostępem do nich osób nieupoważnionych.
4) Pomieszczenia, w których są przetwarzane dane osobowe, są zamykane na klucz.
5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy.
6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W sytuacji, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia administratora danych lub przełożonego.
7) W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
8) Szafy, w których przechowywane są dane, powinny być zamykane na klucz.
9) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.
10) *Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny do wykonania czynności* służbowych, a następnie muszą być chowane do szaf.
11) Dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy.
12) Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane.
13) W razie potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.
14) Nie należy udostępniać osobom nieupoważnionym tych komputerów.
15) W razie potrzeby przeniesienia danych osobowych pomiędzy komputerami należy zrobić to z zachowaniem szczególnej ostrożności.
16) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
17) Jeśli nie ma możliwości skasowania danych z nośnika (np. płyta CD-ROM), należy go zniszczyć fizycznie.
18) W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
19) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
20) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.
21) Hasła dostępu do programów oraz aplikacji muszą posiadać co najmniej 12 znaków, w tym znaki szczególne oraz duże i małe litery.
22) Hasła należy zmieniać nie rzadziej niż co 30 dni.
23) Hasła nie wolno nikomu ujawniać i należy chronić przed dostępem innych osób.
24) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione

niszczone są za pomocą niszczarki.
Za prawidłowy nadzór przetwarzania danych oraz zapewnienie im odpowiedniej ochrony odpowiada każdy pracownik na swoim stanowisku pracy, zgodnie z obowiązkami pracowniczymi.
Za nieprzestrzeganie procedur bezpieczeństwa i naruszenie ochrony danych grozi odpowiedzialność finansowa, odszkodowawcza, dyscyplinarna, a w skrajnych przypadkach nawet karna.
Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia danych osobowych to głównie: 1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp., 2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy, 3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru, 4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów, lub inny komunikat o podobnym znaczeniu, 5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie, 6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych, 7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji), 8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie, 9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń, 10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp., 11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. bocznej furtki itp., 12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane, 13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych itp.).Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.
O każdym przypadku naruszenia lub uzasadnionego podejrzenia naruszenia zabezpieczenia danych osobowych należy bezzwłocznie powiadomić administratora danych.
Uwagi:

Oświadczam, że zapoznałam/em się z treścią instruktażu, w pełni go zrozumiałam/em i zaakceptowałam/em oraz zobowiązuję się stosować do powyższych postanowień, co potwierdzam własnoręcznym podpisem.

Podpis osoby szkolonej: .....

POTWIERDZENIE OBECNOŚCI NA SZKOLENIU „OCHRONA DANYCH OSOBOWYCH „
przeprowadzonym w dniu ..... r. ADMINISTRATOR:.....

Tematyka szkolenia:

1. Omówienie podstawowych zmian dotyczących ochrony danych osobowych osób fizycznych obowiązujących od 25 maja 2018r., na podstawie prawa Unii (ogólne rozporządzenie o ochronie danych z dnia 27 kwietnia 2016r.) oraz prawa krajowego (ustawa z dnia 10 maja 2018 r.)
2. Podstawy prawne przetwarzania danych i obowiązki informacyjne.
3. Zabezpieczenie i ochrona danych osobowych, z uwzględnieniem polityk obowiązujących u administratora.
4. Obowiązek zgłaszania naruszeń i związana z tym procedura postępowania.
5. Odpowiedzialność karna i porządkowa za nieprzestrzeganie przepisów o ochronie danych osobowych.

Niniejszym oświadczam, że byłem uczestnikiem tego szkolenia, w pełni je zrozumiałem i zaakceptowałem. Ponadto zobowiązuję się przestrzegać zasad i przepisów, które zostały mi przedstawione podczas szkolenia.

L.p.	Imię i nazwisko	Podpis
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Szkolący: .....

Załącznik nr 6 do Polityki

REJESTR INCYDENTÓW I NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

L.P.	Naruszenie bezpieczeństwa – opis incydentu/naruszenia	Źródło zgłoszenia – osoba/podmiot zgłaszający incydent/naruszenie	Data zgłoszenia	Przyczyna	Odpowiedzialny za błąd/naruszenie lub informacja o braku takiej osoby	Działanie zapobiegawcze i korygujące wraz ze wskazaniem osoby odpowiedzialnej za wykonanie	Data zakończenia i ocena skuteczności podjętych działań	Czy naruszenie podlegało zgłoszeniu do UODO (TAK/NIE) oraz data zgłoszenia
1.								
2.								
3.								
4.								

....

pieczęć administratora danych osobowych miejscowość, data

Wyznaczenie inspektora ochrony danych

Na podstawie art. 37 ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119/1) - RODO

wyznaczam w .....

Panią/a (imię i nazwisko) .....

do pełnienia od dnia ..... roku funkcji inspektora ochrony danych.

Kontakt mailowy do inspektora: .....

Zakres zadań inspektora określa art. 39 RODO.

Administrator Danych Osobowych

.....

(pieczęć i podpis administratora danych osobowych)

Oświadczam, że przyjmuję powierzoną funkcję.

.....

(data podpis osoby wyznaczonej do pełnienia funkcji IOD)

Załącznik nr 8 do Polityki

Wykaz podmiotów zewnętrznych, którym powierzono dane do przetwarzania.

Lp.	**Nazwa firmy**	**Zakres świadczonych usług**	**Numer/data umowy**	**Uwagi** (czy są zapisy w umowie związane z poufnością i odpowiedzialnością w stosunku do powierzonych danych)
1.				
2.				
3.				
4.				
5.				

Załącznik nr 9 do Polityki

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)(dalej: " RODO") , informujemy, że:

1. **administratorem Państwa danych osobowych jest :**
   Dyrektor Placówek Opiekuńczo – Wychowawczych nr 1,2,3 w Jastrzębiu-Zdroju
2. z administratorem danych osobowych kontaktować można się telefonicznie (32 47 67 406) lub korespondencyjnie wysyłając list na adres:
   Placówka Opiekuńczo -Wychowawcza nr 1 w Jastrzębiu-Zdroju (44-335) , ul. Opolska 7/1-2
3. z inspektorem ochrony danych można kontaktować się korespondencyjnie wysyłając pismo na adres: Placówka Opiekuńczo -Wychowawcza nr 1 w Jastrzębiu-Zdroju (44-335) , ul. Opolska 7/1-2, z dopiskiem "Inspektor Ochrony Danych"
4. dane osobowe przetwarzamy w celu:
   - realizacji obowiązku prawnego (podstawa z art. 6 ust 1 lit. c RODO), wynikającego w szczególności z Ustawy o wspieraniu rodziny i pieczy zastępczej, Ustawy o pomocy społecznej , o pracownikach samorządowych, Ustawy Kodeks pracy, Ustawy o finansach publicznych;
   - zawarcia i wykonania umowy (podstawa z art. 6 ust.1 lit. b RODO);
   - a w szczególnie uzasadnionych przypadkach (np. wizerunek) dane osobowe są przetwarzane na podstawie zgody (podstawa z art. 6 ust. 1 lit. a RODO);
5. dane osobowe udostępniamy organom lub instytucjom upoważnionym z mocy prawa ;
6. dane osobowe są przetwarzane przez okres wymagany przepisami prawa lub przez czas określony w instrukcji kancelaryjnej , a dane osobowe przetwarzane na podstawie zgody są przetwarzane przez okres wskazany w oświadczeniu lub do czasu cofnięcia zgody;
7. w odniesieniu do danych osobowych decyzje nie są podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
8. osoba, której dane dotyczą posiada:
   na podstawie art. 15 RODO prawo dostępu do danych osobowych ,
   na podstawie art. 16 RODO prawo do sprostowania danych osobowych,
   na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO,
   prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna że przetwarzanie danych osobowych jej dotyczących narusza przepisy RODO,
   prawo do cofnięcia zgody -jeżeli dane przetwarzane są na art. 6 ust.1 lit. a RODO;
9. osobie, której dane dotyczą nie przysługuje :
   w związku z art. 17 ust. 3 lit. b), d) lub e) RODO prawo do usunięcia danych osobowych,
   prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
   na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdy podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. c) RODO;
10. administrator danych nie zamierza przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Załącznik nr 10 do Polityki

ARKUSZ ZARZĄDZANIA RYZYKIEM

L.p.	Zagrożenia występujące w związku z planowanymi czynnościami przetwarzania	Poziom ryzyka P x S	Środki zastosowane w celu zaradzenia ryzyku
1.	Utrata danych na skutek działania złośliwego oprogramowania		
2.	Nieuprawniony dostęp osób trzecich, ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe		
3.	Nieuprawnione ujawnienie danych osobom trzecim		
4.	Nieuprawniony dostęp do poczty e-mail		
5.	Kradzież/utrata/zniszczenie teczek oraz nośników elektronicznych zawierających dokumenty, Nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik Utrata nośnika zawierającego dane osobowe. Nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym.		

6.	Awarie oprogramowania , uszkodzenia elementów IT.		
7.	Pożar		
8.	Zalanie		
9.	Przegrzanie, zbyt duża wilgotność		
10.	Błędy i pomyłki Użytkowników		
11.	Awaria zasilania		
12.	Upadek firmy outsourcingowej lub dostawczej		

Uwagi:.....

.....

pieczęć i podpis inspektora ochrony danych osobowych

.....

pieczęć i podpis administratora

OCENA RYZYKA

WYKAZ DZIAŁAŃ NIOSĄCYCH RYZYKO DLA WOLNOŚCI I PRAW OSÓB, KTÓRYCH DOTYCZĄ (zgodnie z wytycznymi Grupy Roboczej 29 - WP 248/2017)

Nazwa czynności przetwarzania:		
l.p.	**Rodzaj działania - czynność polega na lub obejmuje:**	**Czy jest podejmowane?**
1.	ocenę lub punktację w tym profilowanie, lub prognozowanie (na podstawie danych osobowych)	
2.	podejmowanie automatycznych decyzji mających skutki prawne lub w podobny sposób istotnie wpływające na sytuację osoby, której dane dotyczą	
3.	systematyczne monitorowanie, przez które rozumie się przetwarzanie danych w celu obserwowania, monitorowania lub kontroli osób, których dane dotyczą	
4.	przetwarzanie danych wrażliwych – przez takie dane Grupa Robocza rozumie nie tylko dane wskazane w art. 9 RODO, ale też dane dotyczące komunikacji elektronicznej, dane o lokalizacji i dane finansowe	
5.	przetwarzanie danych na dużą skalę	
6.	porównywanie lub łączenie zbiorów danych	
7.	przetwarzanie danych osób wymagających szczególnej ochrony, np. pracowników, dzieci, pacjentów czy osób starszych;	
8.	innowacyjne użycie lub zastosowanie technologicznych lub organizacyjnych rozwiązań, np. połączenie identyfikacji odciskiem palca oraz mechanizmu rozpoznawania twarzy w celu uzyskania dostępu do pomieszczeń, tzw. Internet rzeczy, itp.;	
9.	transgraniczny transfer danych poza Unię Europejską;	
10.	przetwarzanie danych uniemożliwia osobom, których dane dotyczą, korzystanie z praw lub korzystanie z usługi lub umowy	
11.	**Wskazać łącznie sumę czynności z pkt. 1-10, które są podejmowane.**	

Jeżeli w pkt. 11 wykazano więcej niż jedną czynność to Grupa Robocza sugeruje przeprowadzenie oceny skutków dla ochrony danych osobowych. Jednak nie trzeba jej dokonywać, gdy przetwarzanie jest obowiązkiem wynikającym z przepisu prawa lub jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.

OCENA SKUTKÓW OPERACJI PRZETWARZANIA DLA OCHRONY DANYCH ZGODNIE Z ART. 35 RODO

l.p.	**Wymagane elementy oceny**	**Czy jest podejmowane?**
1.	Systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora; ocenę lub punktację w tym profilowanie, lub prognozowanie (na podstawie danych osobowych).	
2.	Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów.	
3.	Wskazanie środków zaplanowanych w celu zaradzenia ryzyku, w tym zabezpieczeń oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych i wykazać przestrzeganie wymagań RODO.	
4.	Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą.	

Jeżeli ocena ryzyka w pkt. 4 wykaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia wolności lub praw osób, których dane dotyczą, a środki zaradcze wskazane w pkt. 3 nie pozwalają na jego zminimalizowanie to należy zrezygnować z danego typu operacji lub rozpocząć uprzednie konsultacje z organem nadzorczym zgodnie z art. 36 RODO.

Protokół z audytu przetwarzania danych osobowych zgodnie z RODO.

Dotyczy zgodności przetwarzania danych osobowych z przepisami o ochronie danych .

1. Przedmiotem sprawdzenia jest zgodność przetwarzania danych osobowych z przepisami Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z 27.04.2016, Ustawą o ochronie danych osobowych z dnia 10.05.2018, Polityką bezpieczeństwa przyjętą przez administratora.
2. Zakres s audytu wraz z opisem stanu faktycznego:

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI	UWAGI
1.	DOKUMENTACJA	Sprawdzenie, czy Polityka Ochrony Danych Osobowych jest aktualna względem obowiązującego stanu prawnego oraz faktycznego.	
2.	DOKUMENTACJA	Sprawdzenie, czy osoba ma upoważnienie do przetwarzania danych osobowych – upoważnienie powinno odzwierciedlać zakres obowiązków.	
3.	DOKUMENTACJA	Sprawdzenie, czy prowadzona jest aktualna ewidencja osób przetwarzających dane osobowe.	
4.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Kontrolowanie osób przetwarzających dane osobowe - czy stosują się do „zasady czystego biurka".	
5.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajdują się szafy zamykane na klucz, w których przechowuje się dokumentację zawierającą dane osobowe podlegające ochronie (jeśli tak - można sporządzić dokumentację fotograficzną pomieszczeń, która stanowić będzie załącznik do poniższego sprawdzenia).	
6.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	*Sprawdzenie, czy w pomieszczeniu znajduje się* niszczarka dokumentów (jeśli takie urządzanie nie znajduje się w pomieszczeniu, należy skontrolować pracownika, w jaki sposób niszczy zbędną dokumentację, która nie podlega archiwizacji). Szczególnie powinno się zwrócić uwagę, czy niepotrzebne dokumenty nie są przypadkiem wyrzucane do kosza na śmieci – dokumenty powinny być niszczone w sposób mechaniczny lub manualny, tak, by uniemożliwić ich odczytanie osobom postronnym.	

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI	UWAGI
7.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, mające na celu sprawdzenie, czy komputer jest zabezpieczony hasłem.	
8.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy systemy komputerowe służące do przetwarzania danych osobowych zapamiętują wszelakie czynności, jakich dokonuje się przy przetwarzaniu danych osobowych.	
9.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Monitorowanie, czy osoby przetwarzające dane osobowe w systemie informatycznym logują się za pomocą WŁASNEGO identyfikatora i hasła.	
10.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie aktywności systemu antywirusowego, na komputerach, które m.in. służą do obsługi systemów przetwarzających dane osobowe.	
11.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, czy pracownik korzysta z wygaszacza ekranu.	
12.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy monitor komputera został usytuowany w sposób uniemożliwiający wgląd do danych - osobom postronnym.	
13.	KONTROLA PRAKTYKI	Przeprowadzenie analizy pod kątem pracowników - jakie obecnie mają problemy w zakresie przetwarzania danych osobowych oraz czy ostatnio miały miejsce zdarzenia typu: 1) próby nieuprawnionego dostępu do danych osobowych 2) działanie zewnętrznych aplikacji, wirusów czy złośliwego oprogramowania; 3) nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym; 4) próba nieuprawnionej interwencji przy sprzęcie komputerowym; 5) wynoszenie niezabezpieczonych pamięci z miejsca pracy; 6) udzielanie informacji osobom postronnym, pomijając formalny tryb administracyjny	

3. Termin audytu.....

4. Inspektor ochrony danych: .....

5. Inne osoby uczestniczące: 1) ..... 2) .....