Załacznik do Zarządzenia Nr 12/2019 Dyrektora ZPO

POLITYKA

OCHRONY DANYCH OSOBOWYCH

ZESPOLE PLACÓWEK OŚWIATOWYCH

w Skarżysku-Kamiennej,

z siedzibą: 26-110 Skarżysko-Kamienna, ul. Zwycięzców 13

Data wprowadzenia:	31/12/ 2019
Wersja:	**Pierwsza**
Daty aktualizacji:	..... / ..... / 2019
Opracowali:	**Agata Dulemba** Inspektor Ochrony Danych **Sebastian Iskra** Radca prawny
Zatwierdził:	**Grażyna Wódz** Dyrektor Zespołu Placówek Oświatowych

(Dokument do użytku wewnętrznego i nie może być udostępniany osobom postronnym w żadnej formie)

SPIS TREŚCI

Spis treści:

WSTĘP

Niniejszy dokument określa zasady zarządzania ochroną danych osobowych **w Zespole Placówek Oświatowych z siedzibą: 26-110 Skarżysko-Kamienna ul. Zwycięzców 13.**

Przetwarzanie danych osobowych przez jednostkę jest ściśle związane z charakterem prowadzonej działalności i wiąże się z realizacją zadań ustawowych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz poprzez użytkowników.

Administrator danych zobowiązany jest do prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz zastosowania środków technicznych i organizacyjnych, na którą składa się Polityka ochrony danych oraz instrukcja zarządzania systemami informatycznymi.

Polityka ochrony danych i instrukcja zarządzania systemem informatycznym są to minimalne zasady ochrony danych osobowych opracowane na podstawie wytycznych i wskazówek Generalnego Inspektora Ochrony Danych Osobowych (obecnie Urzędu Ochrony Danych Osobowych). Na polecenie administratora danych niniejszy dokument może być zmieniany i uzupełniany, w sposób nie skutkujący zmniejszeniem stopnia ochrony danych.

Zasady ochrony danych osobowych określone w niniejszym dokumencie obowiązują od dnia jego zatwierdzenia.

ROZDZIAŁ I

INFORMACJE OGÓLNE

1.Cel polityki ochrony danych osobowych

Zespół Placówek Oświatowych, reprezentowane przez swojego Dyrektora jako Administratora Danych Osobowych (ADO), przetwarza dane osobowe: na podstawie przepisów odnoszących się ściśle do funkcjonowania oświaty. Polityka ochrony danych osobowych została opracowana i wdrożona w strukturze Administratora Danych w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich aktów prawnych, w szczególności:

1. 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),
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2018 r., poz. 1000 ze zm.).

3. Ustawy z dnia 26 stycznia 1982 r. Karta Nauczyciela (tekst jedn. Dz. U .z 2018 r., poz. 967 ze zm.),

4. Ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (tekst jedn. Dz. U. z 2019 r. poz. 1148 ze zm.),

5. Ustawy z dnia 7 września o systemie oświaty (tekst jedn. Dz. U. z 2019 r. poz. 1481),

6. Ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (tekst jedn. Dz. U. z 2019 r. poz. 1942),

7. Ustawy z dnia 27 października 2017 r. o finansowaniu zadań oświatowych (Dz. U. z 2019 r. poz. 1681)

8. oraz rozporządzeń do ww. ustaw, np. rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2017 r. poz. 1646).

Polityka ochrony danych osobowych ma zastosowanie do wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

2.Deklarcja kierownictwa

Dyrektor Zespołu Placówek Oświatowych, jako kierownik jednostki oraz zwierzchnik służbowy w stosunku do pracowników, zgodnie z obowiązującymi wymogami prawa:

a) **w celu ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wdraża** politykę ochrony danych osobowych, która określa w szczególności sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednią do zagrożeń i kategorii danych osobowych objętych ochroną danych osobowych,
b) instrukcję zarządzania system informatycznym, która określa sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
c) oraz deklaruje pełne wsparcie dla podejmowanych działań uzasadnionych realizacją celów zabezpieczenia przetwarzania danych.

9. Terminologia

1. **Administrator Danych (ADO)** – oznacza organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przewarzania danych osobowych –w tym przypadku należy rozumieć: **Zespół Placówek Oświatowych w Skarżysku-Kamiennej, z siedzibą: 26-110 Skarżysko-Kamienna, ul. Zwycięzców 13, reprezentowane przez Dyrektora.**
2. **Administrator Systemów Informatycznych (ASI)** – osoba wyznaczona przez Administratora Danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez Administratora Danych, - w tym przypadku rolę tą pełni **informatyk**, który zajmuje się zabezpieczeniem systemów teleinformatyczny i konserwacją urządzeń do przetwarzania danych.
3. **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
4. **DPIA** – ocena skutków dla ochrony danych osobowych (*data protection impact assessment*),
5. **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora Danych, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych,
6. **organ nadzorczy** – niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO,
7. **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.
8. **podmiot przetwarzający** –osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych,
9. **Polityka** – niniejsza Polityka ochrony danych osobowych,
10. **pracownik** – osoba współpracująca z Administratorem Danych na podstawie umowy o pracę lub umowy cywilnoprawnej,
11. **przetwarzanie** – operacja 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,

12. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
13. **Unia** – Unia Europejska,
14. **Ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.).

4.Zakres informacji objętych polityka ochrony danych osobowych oraz zakres stosowania

1) Polityka ochrony danych ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych u Administratora, niezależnie od formy ich przetwarzania (elektronicznie lub papierowo) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe, tj. księgach, skorowidzach, wykazach i innych zbiorach ewidencyjnych, w szczególności danych osobowych przetwarzanych w celach rekrutacyjnych, zatrudnienia i nawiązania współpracy, finansowych i rachunkowych, marketingowych, handlowych oraz windykacyjnych.
2) Przetwarzane dane u Administratora Danych Osobowych są między innymi informacjami dotyczącymi:
   a) danych osobowych uczniów, dzieci uczęszczających do przedszkola; ich rodziców, nauczycieli, pracowników,
   b) informacji publicznych,
   c) oraz informacji prawnie chronionych.

   Przetwarzane informacje służą do wykonywania zadań statutowych jednostki,
3) Przetwarzanie danych osobowych odbywa się z wykorzystaniem dokumentów, materiałów, przesyłek analogowych (nieelektronicznych), wniosków, pism, akt osobowych pracowników, dokumentów finansowo-księgowych, podań itp. oraz danych zawartych na nośnikach elektronicznych, magnetycznych, optycznych i elektronicznych, w tym przekazywanych drogą elektroniczną, jako załączniki do przesyłek analogowych, a także danych przetwarzanych w systemie kadrowo-płacowym, systemie do obsługi dokumentów ubezpieczeniowy i wymianie informacji z ZUS, systemie teleinformatycznym administracji.
4) Dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Szkoła/ Przedszkole może żądać podania jedynie tych danych, które są niezbędne do realizacji jej celów i zadań.
5) Zakres danych osobowych przetwarzanych przez jednego Użytkownika w systemie IT nie może być szerszy niż powierzony do przetwarzania w związku z wykonywanymi przez niego obowiązkami.
6) Po wykorzystaniu, dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą, zniszczone lub, w przypadku powierzenia, zwrócone podmiotowi, który dane powierzył.
7) Politykę ochrony danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia

danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Polityce.

8) Rygorowi Polityki podlegają także dane powierzone Administratorowi Danych do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi Danych udostępnione.
9) Ochrona danych osobowych u Administratora Danych dotyczy w szczególności:
   a) danych osobowych wytworzonych (gromadzonych, przetwarzanych) w związku z działalnością Administratora Danych, w tym danych osobowych uczniów/dzieci, rodziców (opiekunów prawnych) i kontrahentów oraz współpracowników w związku z zawieranymi umowami,
   b) danych osobowych pracowników, w tym danych osobowych i treści zawieranych umów o pracę,
   c) danych osobowych kandydatów do pracy zbieranych na etapie rekrutacji,
   d) danych osobowych zawartych w kartach zapisu ucznia/dziecka do szkoły/przedszkola.
   e) danych osobowych zawartych w dokumentach finansowo-księgowych,
   f) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach IT, w których są przetwarzane dane osobowe,
   g) danych osobowych zawartych w rejestrze osób dopuszczonych do przetwarzania danych osobowych stosownie do ustawy o ochronie danych osobowych,
10) Z uwagi na rodzaj i charakter danych osobowych zawartych w zbiorach u Administratora Danych identyfikuje się następujące przypadki przetwarzania danych:
   a) ***dane osobowe zwykłe*** – dane osobowe niezbędne do wykonania zadań administratora danych odnoszących się do uczniów, ich rodziców oraz zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w przepisach odnoszących się ściśle do funkcjonowania oświaty (np. w ustawie Prawo oświatowe, Karta Nauczyciela) ,
   b) ***dane szczególnych kategorii danych osobowych i dane karne*** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, których przetwarzanie jest dopuszczalne w związku z art. 9 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). Całość procesu przetwarzania opiera się o przesłanki określone w art. 9 ust. 2 i art. 10 RODO.
   c) ***dane niezidentyfikowane*** - do głównych procesów przetwarzania danych niezidentyfikowanych dochodzi w ramach stosowanego monitoringu wizyjnego, którego reguły działania ustala odrębna instrukcja postępowania dostępna na stronie jednostki oraz w miejscach oznaczonych tabliczką informującą o objęciu terenu czy pomieszczeń monitorowaniem.

11) Wykaz zbiorów danych osobowych, których administratorem jest Zespół Placówek Oświatowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. stanowi **Załącznik nr 3** do Polityki.
12) **Do zasobu informatycznego** Zespołu Placówek Oświatowych **zalicza się:**
    a) zbiory danych przetwarzane za pośrednictwem sytemu informatycznego,
    b) zasoby programowe zastosowane do przetwarzania danych za pośrednictwem danego sytemu informatycznego,
    c) oraz zasoby sprzętowe do których zalicza się: komputery przenośne, komputery stacjonarne, urządzenia mobilne, drukarki, sprzęt sieciowy (np. ruter), monitory, sprzęt serwerowy, osprzęt zakupiony łącznie lub osobno, np. myszki, zasilacze.
13) Przetwarzanie danych osobowych u Administratora danych odbywa się na stacjach roboczych użytkowników przy wykorzystaniu programów, systemów wspomagających pracę i zarządzanie oraz funkcjonowanie Szkoły/Przedszkola. Wykaz programów, systemów wspomagających pracę oraz zarządzanie i funkcjonowanie Zespołu Placówek Oswiatowych, **stanowi załącznik nr 8 do Polityki.**
14) Zbiory danych osobowych przetwarzane za pośrednictwem systemu informatycznego zawiera wykaz zbiorów danych, stanowiący **załącznik nr 3 do Polityki**.

ROZDZIAŁ II

PODSTAWOWE OBOWIĄZKI ORAZ ODPOWIEDZIALNOŚĆ OSÓB BIORĄCYCH UDZIAŁ W PROCESIE PRZETWARZANIA DANYCH OSOBOWYCH

W celu skutecznego zarządzania ochroną danych osobowych u Administratora Danych Osobowych, w zakresie ochrony danych osobowych tworzy następującą strukturę organizacyjną :

1. Administrator Danych Osobowych,
2. Inspektor Ochrony Danych,
3. Administrator Systemów Informatycznych,
4. Osoby upoważnione do przetwarzania danych osobowych.

1. Administrator Danych Osobowych

1) Administratorem danych (ADO) uczniów/ dzieci przyjętych do szkoły, przedszkola ich rodziców, nauczycieli, pracowników jest Zespół Placówek Oświatowych, reprezentowany przez Dyrektora, który ustala cele i sposoby przetwarzania danych osobowych oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.
2) Administrator Danych wyznacza:
    a) Inspektora Ochrony Danych,
    b) Administratora Systemów Informatycznych.
3) Administrator Danych jest odpowiedzialny za:

a) zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,
b) wdrożenie odpowiednich procedur ochrony danych osobowych,
c) zapewnienie środków umożliwiających prawidłowa realizację praw osób, których dane dotyczą,
d) prowadzenie rejestru czynności przetwarzania danych osobowych,
e) prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,
f) współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,
g) przeprowadzanie analizy ryzyka oraz w razie konieczności opracowanie oceny skutków dla ochrony danych,
h) wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
i) zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,
j) dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,
k) nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
l) zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,
m) w stosunku do Inspektora Ochrony Danych (IOD):
   - zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
   - wspieranie IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,
   - zagwarantowanie by IOD nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,
   - publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.

2.Inspektor Ochrony Danych

1) Funkcję Inspektora Ochrony Danych pełni osoba wyznaczona przez Administratora Danych. Wzór dokumentu wyznaczenia oraz odwołania IOD znajduje się w **Załączniku nr 1** do Polityki.

2) Inspektor ochrony danych (IOD) wykonuje zadania określone art. 39 Rozporządzenia RODO, tj. :
   a) informuje administratora oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach na nich spoczywających na mocy przepisów rozporządzenia oraz innych przepisów z zakresu ochrony danych osobowych,

b) monitoruje przestrzeganie przez pracowników placówki ochrony danych osobowych miedzy innymi poprzez:
   - przygotowywanie pod podpis administratora upoważnień (pracownikom, stażystom, wolontariuszom, praktykantom) zgodnie z podziałem obowiązków, według wzoru określonego w Polityce,
   - prowadzenie ewidencji wydanych upoważnień do przetwarzania danych osobowych; ewidencja powinna zawierać: imię i nazwisko osoby upoważnionej; data nadania i ustalania oraz zakres upoważnienia do przetwarzania danych osobowych; identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
   - prowadzenie rejestru zbiorów danych osobowych przetwarzanych u administratora; w ramach prowadzenia rejestru; wpisuje zbiór danych do rejestru przed rozpoczęciem jego przetwarzania, aktualizuje informacje dotyczące zbioru (zmiana informacji objęta wpisem – rodzaj zmiany, np. nowy wpis, aktualizacja, wykreślenie), datę dokonania zmiany, informacje o zakresie zmiany), wykreśla zbiór z rejestru (w przypadku zaprzestania przetwarzania w nim danych), udostępnia rejestr do przeglądania w siedzibie Zespołu Placówek Oświatowych.
   - prowadzenie szkoleń z zakresu ochrony danych osobowych,
   - prowadzenie ewidencji zawartych umów powierzenia danych osobowych,
   - przeprowadzanie sprawdzeń (kontroli) zgodności przetwarzania danych osobowych z Ustawą i Rozporządzeniem oraz wewnętrznymi regulacjami oraz opracowuje w tym zakresie sprawozdania, które przedkłada administratorowi;
   - w przypadku wykrycia nieprawidłowości powstałych podczas przetwarzania danych, zawiadamia administratora, poucza lub instruuje osobę nieprzestrzegającą zasad określonych w dokumentacji przetwarzania danych o prawidłowym sposobie ich realizacji, wskazuje osobę odpowiedzialną za naruszenie tych zasad oraz jego zakres.

c) w imieniu administratora pełni rolę tzw. punktu kontaktowego, we wszystkich sprawach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem praw przysługujących osobom, których dane dotyczą (art.38 ust.4 Rozporządzenia RODO) .

d) jako – przedstawiciel administratora prowadzi w jego imieniu rejestr czynności lub kategorii czynności przetwarzania oraz udostępnia go na żądanie organu nadzorczego. (art. 30 Rozporządzenia RODO).

e) udzielanie na żądanie administratora zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

f) współpraca z organem nadzorczym,

g) opracowuje i aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednia do zagrożeń oraz kategorii danych objętych ochroną – poprzez: zgodność dokumentacji z obowiązującymi przepisami prawa oraz stanem faktycznym w zakresie przetwarzania danych.

3) W celu realizacji swoich zadań inspektor:

a) posiada pełny dostęp do wszystkich danych osobowych przetwarzanych w Zespole Placówek Oświatowych, a także do pomieszczeń placówki, w których przetwarzane są dane osobowe. Dostęp do pomieszczeń odbywa się przy udziale osób upoważnionych do przetwarzania danych osobowych,.

b) kontroluje poszczególne stanowiska pracy w zakresie właściwego przestrzegania procedur ochrony informacji oraz pomieszczenia, w których przetwarzane są dane osobowe.
c) wydaje polecenia pracownikom zatrudnionym w Szkole/Przedszkolu w zakresie bezpieczeństwa danych osobowych.
d) informuje administratora o przypadkach naruszenia bezpieczeństwa danych osobowych.
e) żąda od pracowników Szkoły/Przedszkola wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

3. Administrator Systemu Informatycznego

1) Funkcję Administratora Systemu Informatycznego pełni informatyk zatrudniony u Administratora Danych, który zajmuje się zarządzaniem systemem informatycznym oraz odpowiada za jego sprawne działanie.
2) Jako administrator systemu informatycznego – informatyk - odpowiada za bezpieczeństwo danych osobowych przetwarzanych za pomocą systemów informatycznych w sposób gwarantujący utrzymanie poufności, dostępności i integralności gromadzonych w nich danych na poziomie pozwalającym zachować zgodność z wymogami prawnymi i organizacyjnymi.
3) Do najważniejszych zadań informatyka należy:
   a) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,, w tym zabezpieczenie zbiorów danych oraz programów służących do przetwarzania danych osobowych poprzez systematyczne wykonywanie kopii zapasowych.
   b) sporządzanie i zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
   c) dbałość, aby wykonane kopie zapasowe przechowywać w miejscu zabezpieczającym je przed nieuprawnionym dostępem , modyfikacją, uszkodzeniem lub zniszczeniem,
   d) optymalizacja wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego, instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
   e) konfigurowanie i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieuprawnionym dostępem, w tym bieżące rejestrowanie i wyrejestrowywanie użytkowników z systemu.
   f) współpraca z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych w umowach serwisowych,
   g) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
   h) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   i) zarządzanie licencjami oraz procedurami ich dotyczącymi,
   j) prowadzenie profilaktyki antywirusowej - zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego, którego celem może okazać się uzyskanie nieuprawnionego dostępu do danych.
   k) zapewnienie awaryjnego źródła zasilania oraz zabezpieczenia przed zakłóceniami w sieci zasilającej systemów informatycznych służących do przetwarzania danych osobowych, których nagła przerwa w pracy mogłaby spowodować utratę danych lub naruszenie ich integralności.

l) nadzór nad naprawą oraz likwidacją urządzeń komputerowych,
m) sprasowuje nadzoru nad kopiami zapasowymi,
n) prowadzenie rejestru nadanych uprawnień do systemów informatycznych,
o) opracowywanie oraz aktualizacja opisu technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych,

4) Informatyk ściśle współpracuje z Inspektorem Ochrony Danych w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych poprzez:
a) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
b) identyfikację i analizę zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
c) inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,

5) Administrator Systemu Informatycznego posiada pełny dostęp do danych osobowych znajdujących się w systemach informatycznych oraz do instalacji informatycznej, systemów i urządzeń znajdujących się u Administratora Danych za pomocą, których przetwarzane są dane osobowe. Posiada również pełny dostęp do wszystkich pomieszczeń Administratora Danych, w którym ulokowany jest sprzęt informatyczny oraz okablowanie strukturalne.

10. Osoba upoważniona do przetwarzania danych osobowych

1) W celu osiągnięcia i utrzymania **wysokiego poziomu** bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego uczestnika w proces ochrony danych osobowych.
2) Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki.
3) Dostęp do zbiorów danych osobowych oraz ich przetwarzania mają tylko osoby, które posiadają pisemne upoważnienie oraz uprawnienia do przetwarzania danych osobowych wydane przez Administratora, zobowiązały się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobu ich zabezpieczenia oraz zapoznały się z Polityką Ochrony Danych Osobowych.
4) Obowiązek do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór stanowi **załącznik nr 2 do Polityki.**
5) Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974r. Kodeks Pracy (tekst jedn. Dz.U. z 2019r., poz. 1040.), bądź rozwiązania stosunku cywilnoprawnego.
6) Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do przestrzegania następujących zasad:

a) może przetwarzać dane osobowe wyłącznie w celu wykonywania nałożonych na nią obowiązków służbowych zgodnych z posiadanym zakresem czynności; rozwiązanie stosunku pracy lub odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych,
b) musi zachować w tajemnicy dane osobowe oraz przestrzegać procedur ich bezpiecznego przetwarzania; przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia , a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,
c) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Ochrony Danych Osobowych oraz instrukcji zarządzania systemem informatycznym,
d) stosuje określone przez Administratora Danych Osobowych procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych,
e) korzysta z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników,
f) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym,
g) zabezpiecza indywidualne hasła dostępu do zbiorów danych osobowych przed dostępem osób trzecich,
h) uczestniczenie w szkoleniach z zakresu bezpieczeństwa informacji,
i) procedur związanych z otwieraniem i zamykaniem pomieszczeń, w których następuje przetwarzanie danych, a także nadzorowanie wejść do obszarów przetwarzania danych osobowych osób nieupoważnionych,
j) archiwizowania na bieżąco dokumentacji, zgodnie z obowiązującymi przepisami kancelaryjno-archiwalnymi.

7) Administrator Danych dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.

ROZDZIAŁ III

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1.Ogólne zasady przetwarzania danych osobowych

1) Przetwarzanie danych osobowych przez Zespół Placówek Oświatowych jest ściśle związane z charakterem prowadzonej działalności i wiąże się z realizacją zadań ustawowych, wynikających ściśle z prowadzonej działalności oświatowej.
2) Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:
   a) zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazana w art. 6 lub 9 RODO) – **zasada „legalności”,**
   b) rzetelnie przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą – **zasada „rzetelności”,**
   c) w sposób przejrzysty dla osoby, której dane dotyczą – **zasada „przejrzystości”,**
   d) zbierane dane przetwarza się w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami – **zasada „ograniczenie celu”**,
   e) w zakresie adekwatnym, stosownym oraz niezbędnym do celów, w których są przetwarzane – **zasada „minimalizacji danych”,**
   f) przy uwzględnieniu ich prawidłowości i w razie potrzeby ich uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane – **zasada „prawidłowości”**,
   g) poprzez przechowywanie w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą – **zasada „ograniczenie przechowywania”,**
   h) 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 – **zasada „integralności i poufności**.
   i) z **zasadą „rozliczalności”** poprzez wykazanie przez Administratora Danych obowiązku przestrzegania ww. zasad.

3) Administrator Danych gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

2. Zgodność z prawem przetwarzania danych osobowych u Administratora

1) W Zespole Placówek Oświatowych dopuszczalne jest tylko przetwarzanie danych zgodnie z prawem, po spełnieniu co najmniej jednego z poniższych warunków:
   a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   b) 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;
   c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze Danych;
   d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;
   e) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych, 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.
2) Dane muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada zgodności z prawem, rzetelności i przejrzystości).
3) Dane muszą być zbierane w konkretnych, wyraźnych, prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami (zasada ograniczenia celu).
4) Dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych).
5) Dane muszą być prawidłowe i w razie potrzeby uaktualniane; w przypadku danych osobowych, które są nieprawidłowe w świetle celów ich przetwarzania, muszą być niezwłocznie usunięte lub sprostowane (zasada prawidłowości).
6) Dane muszą być 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożono odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą (zasada ograniczonego przechowywania).
7) Dane muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym, niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (zasada integralności i poufności).

8) W przypadku przetwarzania na podstawie zgody, AD musi być wstanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Zgoda musi być wyrażona dobrowolnie.
9) W przypadku wyrażenia zgody przez osobę, której dane dotyczą, w pisemnym oświadczeniu, zapytanie o zgodę musi być przedstawione w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
10) Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
11) W przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.
12) **Administrator Danych jest uprawniony do przekazywania zebranych przez siebie danych osobowych organom je prowadzącym, gdyż wiąże się to z wykonywaniem przez nie swoich kompetencji lub obowiązków określonych przepisami prawa**. Zespół Placówek Oświatowych **zapewnia dostęp do danych osobowych (informacji) organowi prowadzącemu do przetwarzanych danych w związku z realizacją swoich obowiązków wynikających z przepisów prawa**.

Administrator Danych wprowadza i zobowiązuje wszystkich przetwarzających dane do ich przetwarzania, zgodnie z poniżej opisanymi procedurami (zasadami):

- **zasada zgodności z prawem, rzetelności i przejrzystości**: przetwarzamy dane osobowe w sposób zgodny z przepisami prawa. O wszystkich kwestiach z tym związanych informujemy wyczerpująco ustalonymi kanałami komunikacji i jak najprostszym językiem, by osoby, których dane dotyczą, były świadome, że zbieramy, przechowujemy lub w inny sposób przetwarzamy ich określone dane osobowe;
- **zasada minimalizacji i adekwatności danych**: przetwarzamy tylko te dane (adekwatne, stosowne), które są rzeczywiście potrzebne, by zrealizować dany cel;
- **zasada prawidłowości danych**: dokładamy najwyższej staranności, by dane, które przetwarzamy, były zgodne z prawdą, aktualne i dokładne. Dlatego możemy co jakiś czas prosić osoby, których dane przetwarzamy, o to, by sprawdziły i zaktualizowały swoje dane. Prosimy ich też o to, by klienci informowali nas o wszelkich zmianach swoich danych osobowych (imię i nazwisko, adres itp.);
- **zasada ograniczenia celu oraz przechowywania przetwarzanych danych**: dane osobowe zbieramy jedynie w konkretnym, wyraźnym i prawnie uzasadnionym celu, którego nie moglibyśmy osiągnąć w inny sposób. Przechowujemy dane w formie, która uniemożliwia identyfikację osoby, której dane dotyczą. Przetwarzamy je tylko tak długo, jak jest to niezbędne, by zrealizować cel, dla którego je pozyskaliśmy (chyba, że do dalszego przetwarzania zobowiązują nas przepisy prawa);
- **zasada integralności i poufności danych**: zapewniamy takie rozwiązania informatyczne i organizacyjne, dzięki którym dane osobowe, które przetwarzamy, są bezpieczne. Chronimy dane przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem;

- **zasada rozliczalności**: jesteśmy w stanie wykazać (w sposób, w jaki wymaga od nas prawo), że w odniesieniu do danych osobowych działamy zgodnie z przepisami prawa, uwzględniamy ochronę danych w fazie projektowania (np. nowego zadania, projektu) oraz zapewniamy domyślną ochronę danych osobowych.

3. Dopuszczenie osób do przetwarzania danych osobowych

1) Administrator Danych realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.
2) Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych.
3) Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.
4) Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi **Załącznik nr 4 do Polityki.**
5) **Administrator Danych Osobowych określa procedurę nadawania, modyfikowania oraz odbierania upoważnień i uprawnień do przetwarzania danych osobowych:**
   a) do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające indywidualne upoważnienie oraz uprawnienia do systemu - zakres nadanego upoważnienia wynika z zakresu obowiązków pracowniczych,
   b) w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych,
   c) wszystkie osoby upoważnione do przetwarzania danych osobowych muszą podpisać oświadczenie o zapoznaniu się z przepisami o ochronie danych osobowych oraz zachowaniu poufności danych osobowych. ***Wzór oświadczenia o zachowaniu poufności danych stanowi załącznik nr 5 do Polityki.***
   d) podpisane oświadczenie o zachowaniu poufności danych wraz z upoważnieniem przechowuje się w aktach osobowych pracownika, lub w dokumentacji stażysty, praktykanta – prowadzonej przez Sekretarza Szkoły ~~Dorotę~~ Winiarską.
   e) pracownik, któremu zostanie zmienione upoważnienie lub uprawnienie, powinien uzyskać nowe upoważnienie (lub uprawnienie) przed podjęciem pierwszej czynności dotyczącej przetwarzania danych we wnioskowanym zakresie,
   f) **Upoważnienie** oraz nadane uprawnienie do przetwarzania danych osobowych wygasa obligatoryjnie, w przypadku :
      - upływu terminu, na jaki zostało wydane,
      - przesunięcia pracownika na inne stanowisko pracy,
      - zmiany imienia lub nazwiska Użytkownika,
      - rozwiązania stosunku pracy, w tym zakończenia stażu, praktyki,
      - wygaśnięcia lub rozwiązania umowy cywilnoprawnej zawartej z osobą fizyczną.
   g) Administrator Danych Osobowych w każdym czasie może odwołać(cofnąć) upoważnienie lub w przypadku uzasadnionego wniosku IOD, informatyka lub z chwilą

powzięcia informacji o wystąpieniu realnego wystąpienia zagrożenia danych osobowych przetwarzanych przez upoważnionego lub użytkowania systemu informatycznego.

h) po wygaśnięciu nadanego upoważnienia do przetwarzania danych osobowych informatyk zablokuje konto użytkownika w systemie informatycznym, w którym były przetwarzane dane osobowe.

i) rejestr (ewidencję) osób upoważnionych do przetwarzania danych osobowych prowadzi Sekretarz Szkoły – **zgodnie z załącznikiem nr 4 do Polityki.**

Dostęp organu prowadzącego do danych

1. Organ prowadzący placówkę oświatowa ma dostęp do danych osobowych przetwarzanych w szkole/przedszkolu w związku z realizacją swoich obowiązków wynikających przepisów prawa, m.in. do danych osobowych nauczycieli zawartych w arkuszu organizacji placówki (imion, nazwisk, stopni awansu zawodowego, kwalifikacji poszczególnych nauczycieli oraz rodzajów prowadzonych przez nich zajęć, w tym godzin tych zajęć).
2. Placówka przekazuje dane osobowe organowi prowadzącemu w postaci papierowej lub elektronicznej, jeżeli takie działanie na odpowiednią podstawę prawną. Organ prowadzący przetwarza dane pozyskane dane w sposób zapewniający ich bezpieczeństwo.
3. Dostęp organu prowadzącego do danych osobowych musi być adekwatny do celu przetwarzania danych, co oznacza, ze zakres udostępnianych danych musi być odpowiedni (bez nadmiaru) do celu przetwarzania – zgodnie z zasadą minimalizacji danych.
4. W przypadku kontroli przeprowadzanej przez organ nadzoru , zgodnie z art. 29 i 32 ust. 4 RODO osoba kontrolująca musi posiadać upoważnienie organu prowadzącego do przeprowadzenia kontroli, w którym winien być określony zakres kontroli. Przed udostępnieniem danych organowi prowadzącemu na potrzeby kontroli, placówka rozważa, czy żądany zakres danych nie jest zbyt szeroki w stosunku do celu kontroli.

4. Powierzenie przetwarzania danych osobowych

1) Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2) Powierzenie przetwarzania danych osobowych przez Administratora Danych Osobowych innemu podmiotowi przetwarzającemu następuje na podstawie umowy powierzenia lub innego aktu prawnego, zawartej w trybie art. 28 ust.9 RODO w formie pisemnej, w tym w formie elektronicznej.
3) Podmiot, z którym zostaje zawarta umowa powierzenia jest zobowiązany do wdrożenia środków organizacyjnych i technicznych odpowiednich do ryzyk przetwarzania powierzonych danych, zabezpieczenia powierzonego zbioru przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych, prowadzenia rejestru czynności przetwarzania, zgłaszania naruszeń ochrony danych do organu nadzorczego, czyli Prezesa Urzędu Ochrony Danych Osobowych.

4) Podmiot przetwarzający, o którym mowa w pkt. 3, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.
5) Za przygotowanie umowy powierzenia danych osobowych odpowiada pracownik merytoryczny, który planuje zlecać wykonanie zadania do realizacji podmiotowi zewnętrznemu. Pracownik ten przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez IOD.
6) Ostateczna decyzje, co do powierzenia danych osobowych firmie zewnętrznej podejmuje Dyrektor, który zawiera (jako Administrator Danych) umowę powierzenia przetwarzania danych osobowych. Umowa musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:
   a) przedmiot powierzenia,
   b) czas trwania powierzenia,
   c) charakter i cel przetwarzania,
   d) rodzaj powierzanych danych osobowych,
   e) kategorie osób, których dane dotyczą,
   f) warunki podpowierzenia przetwarzania danych,
   g) obowiązki i prawa Administratora Danych,
   h) obowiązki podmiotu przetwarzającego.

   Wzór umowy powierzenia, zgodny z art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych, stanowi **załącznik nr 6 do Polityki**.
7) W przypadku, w którym podmiot zewnętrzny określony w umowie powierzenia danych osobowych, w zakresie realizacji swoich usług korzysta z pomocy innych podmiotów (podpowierzenie danych), wymagana jest zgoda Administratora Danych Osobowych na przekazanie powierzonych danych, wyrażona w formie pisemnej.
8) W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w pkt 6) znajdują się już w zawartej z danym podmiotem umowie (tzw. umowa podstawowa), nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.
9) Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora Danych lub udzielonymi pełnomocnictwami.
10) Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych oraz w wykazie podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi. Wzór rejestru czynności przetwarzania danych osobowych – **stanowi załącznik nr 7 do Polityki,** natomiast wzór wykazu podmiotów, którym powierzono dane osobowe stanowi **załącznik nr 9 do Polityki**
11) Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych.

12) Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

13) **W celu realizacji obowiązku wymienionego w pkt. 10 Administrator Danych zobowiązuje wszystkich pracowników do obligatoryjnego przekazywania kopii zawartych umów powierzenia z podmiotami zewnętrznemu do sekretariatu Dyrektora.**

14) Fakt powierzenia danych osobowych podmiotowi zewnętrznemu odnotuje w prowadzonym rejestrze oraz wykazie (wymienionym w pkt. 10) prowadzonym w imieniu ADO przez Sekretarza Szkoły.

15) Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

5. Udostępnianie danych osobowych

1) Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.
2) Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której administrator danych udostępniający dane oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności.
3) Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.
4) Udostępnianie danych osobowych może nastąpić w następujących przypadkach :
   a) wynikających z przepisów prawa oświatowego,
   b) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów,
   c) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych,
   d) na podstawie wniosku osoby, której dane dotyczą.
5) Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.
6) Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
7) W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą – odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.
8) **Fakt udostępnienia danych osobowych ze zbiorów tradycyjnych odnotowuje w dokumentacji udostępnień danych osobowych,**

9) Informacje o odbiorcach, którym udostępniono dane osobowe przetwarzane w systemie informatycznym powinny być automatycznie odnotowane w systemie (zakres udostępnienia, data).

Udostępnianie danych osobowych uczniów dla potrzeb realizacji opieki zdrowotnej przez pielęgniarkę szkolną, lekarza i lekarza stomatologa

1) Zgodnie z art. 68 ust. 1 pkt 11) ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe, Dyrektor szkoły współpracuje z pielęgniarką albo higienistką szkolną, lekarzem i lekarzem dentystą, sprawującymi profilaktyczną opiekę zdrowotną nad dziećmi i młodzieżą, w tym celu udostępnia imię, nazwisko i numer PESEL ucznia celem właściwej realizacji tej opieki.
2) Zakres udostępnianych danych przez Szkołę nie może ulec rozszerzeniu. Mając powyższe na względzie Administrator Danych stwierdza, iż nie zachodzą przesłanki do tego, aby zawierać umowy powierzenia przetwarzania danych z podmiotami leczniczymi.
3) Dyrektor Szkoły wskazuje pomieszczenie, którym będzie przechowywana dokumentacja medyczna. Oobowiązek właściwego przechowywania dokumentacji medycznej ciąży na podmiocie świadczącym opiekę zdrowotną w szkole.

Udostępnianie danych osobowych uczniów samorządowi uczniowskiemu

1) Zgodnie art. 68 ust. 2 - Prawa oświatowego dyrektor szkoły udostępnia dane osobowe uczniów innym uczniom (niepełnoletnim) wchodzącym skład samorządu uczniowskiego w celu wydania opinii, np. w związku ze skreśleniem ucznia z listy uczniów w przypadkach określonych w Statucie Szkoły.
2) Przetwarzanie przez przedstawicieli samorządu uczniowskiego danych ucznia, który ma zostać skreślony z listy następuje na podstawie wyraźnego upoważnienia ustawowego.
3) Członkowie samorządu szkolnego są zobowiązani do zachowania poufności przetwarzanych danych, zatem **nie jest dopuszczalne przekazanie danych** przez członków samorządu innemu podmiotowi.

6. Przekazywanie danych do państw trzecich lub organizacji międzynarodowych

1) Przekazywanie danych, których Administratorem Danych jest do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V Rozporządzenia 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).
2) Szkoła/Przedszkole co do zasady nie przekazuje danych osobowych do państw trzecich, niemniej jednak przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych, co oznacza, że w zależności od rodzaju przekazania, należy wziąć również pod uwagę postanowienia podrozdziałów 4 i 5 Polityki.
3) Przekazanie danych osobowych, których administratorem jest Administrator Danych do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo

trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

7. Współadministrowanie danymi osobowymi

1) Administrator Danych w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.
2) Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator Danych oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie przetwarzania danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator Danych oraz co najmniej jeden inny podmiot muszą:
   a) być administratorami w rozumieniu art. 4 pkt 7 RODO,
   b) muszą wspólnie ustalić cele przetwarzania danych,
   c) muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.
3) W przypadku spełnienia warunków, o których mowa w pkt. 2 Administrator Danych oraz co najmniej jeden inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.
4) W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.
5) W sytuacji, kiedy w zakresie zachodzących w strukturze Administratora Danych procesów przetwarzania danych osobowych pojawią się procesy wobec których istnieje prawdopodobieństwo zachodzenia współadministrowania danymi, każdy upoważniony informuje o tym fakcie IOD. IOD dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania danymi.
6) W przypadku, kiedy wynik oceny, o której mowa w pkt. 5 wskazuje na współadministrowanie danymi osobowymi, IOD, przy współudziale pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w pkt. 4.

8. Sprawdzenia (audyt) zgodności przetwarzania danych osobowych

1) Sprawdzenia (audyty) zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych przeprowadzane są przez IOD.
2) Odbiorcą sprawdzeń jest Administrator Danych Osobowych lub w określonych przypadkach Urząd Ochrony Danych Osobowych.
3) Inspektor ochrony danych przeprowadza sprawdzenia w trybie:
   a) sprawdzenia planowego – według planu sprawdzeń przedstawionego administratorowi danych,
   b) sprawdzenia doraźnego - w przypadku pozyskania informacji o naruszeniu ochrony danych, lub uzasadnionego podejrzenia wystąpienia takiego naruszenia,

c) na wniosek Urzędu Ochrony Danych Osobowych.

4) Inspektor ochrony danych przygotowuje plan sprawdzeń na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan obejmuje co najmniej jedno sprawdzenie i jest przedstawiany ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu nim objętego.
5) Zbiory danych oraz system informatyczny służący do przetwarzania lub zabezpieczania danych osobowych są obejmowane sprawdzeniem co najmniej raz na pięć lat.
6) Inspektor ochrony danych zawiadamia Administratora Danych o rozpoczęciu sprawdzenia doraźnego lub na wniosek Urzędu Ochrony Danych Osobowych.
7) IOD dokumentuje czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i opracowania sprawozdania.
8) Dokumentowanie czynności w toku sprawdzenia może polegać na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczenia danych osobowych na elektronicznym nośniku danych lub dokonaniu wydruków tych danych oraz na:
   a) Sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń oraz systemów informatycznych służących do przetwarzania danych osobowych,
   b) Odebrania wyjaśnień od osoby, której czynności objęto sprawdzeniem,
   c) Sporządzenie kopii otrzymanego dokumentu,
   d) Sporządzenie kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczenia danych osobowych,
9) Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze udział w sprawdzeniu lub umożliwia IOD przeprowadzenie czynności w toku sprawdzenia.
10) Po zakończeniu sprawdzenia inspektor ochrony danych przygotowuje ADO sprawozdanie:
   a) ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia,
   b) ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia,
   c) sprawdzenie na zlecenie Urzędu Ochrony Danych Osobowych – zachowuje wskazany termin.

9. Sprawozdanie roczne stanu systemu ochrony danych osobowych

Corocznie Inspektor Ochrony Danych przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych u Administratora Danych. Sprawozdanie przygotowywane jest w formie pisemnej.

10. Realizacja praw osób, których dane dotyczą

1) Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:
   a) prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
   b) prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),

c) prawo do sprostowania danych (art. 16 RODO),
d) prawo do usunięcia danych (*prawo do bycia zapomnianym*) (art. 17 RODO),
e) prawo do ograniczenia przetwarzania (art. 18 RODO),
f) prawo do przenoszenia danych (art. 20 RODO),
g) prawo sprzeciwu (art. 21 RODO),
h) prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).
i) prawo o poinformowaniu o naruszeniu ochrony danych osobowych (art. 34 RODO),
j) prawo do informacji na temat przetwarzanych danych (art. 13 i 14 RODO).

2) **W celu zapewnienia realizacji praw osób, których dane dotyczą oraz realizacji obowiązków Administratora Danych Osobowych względem tych osób** - zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. 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) oraz Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. – Dyrektor Zespołu Placówek Oświatowych (reprezentujący Administratora Danych), **zobowiązuje pracowników do stosowania zasad postępowania z danymi osobowymi poprzez :**
   a) wypełnienie obowiązku informacyjnego wynikającego z art. 13 i 14 RODO – przekazywanie informacji na temat przetwarzanych danych osobowych, zgodnie procedurą realizacji praw osób, których dane dotyczą została opisana w pkt.15 Polityki „Obowiązek informacyjny",
   b) prawa realizowane na wniosek osób, których dane dotyczą (art.15-21 RODO):

- **w przypadku prawa dostępu** (art.15 RODO) przysługujące osobie, której dane dotyczą uzyskanie potwierdzenia, czy w Szkole/Przedszkolu przetwarzane są jej dane osobowe. Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz pozyskania następujących informacji:
  - ✓ w jakim celu są przetwarzane jej dane osobowe,
  - ✓ jakich kategorii danych osobowych dotyczy przetwarzanie,
  - ✓ o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
  - ✓ o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu,
  - ✓ o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
  - ✓ o prawie wniesienia skargi do organu nadzorczego,
  - ✓ o źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą.

Oprócz informacji, o których mowa powyżej osoba, której dane dotyczą może zwróci się z wnioskiem **o dostarczenie kopii jej danych osobowych** podlegających przetwarzaniu żądanie takie realizuje się bezpłatnie. Za wszelkie kolejne kopie, o które zwróci się ta osoba, można pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zaznacza we wniosku w jakim formacie chce otrzymać kopię danych (drogą elektroniczną lub tradycyjną).

- **w przypadku prawa do sprostowania danych** (art. 16 RODO) osoba, której dane dotyczą, ma prawo :
  - ✓ żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe,
  - ✓ żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Wniosek o sprostowanie lub uzupełnienie danych przekazywany jest w formie pisemnej lub drogą elektroniczną na adres Szkoły/Przedszkola. Pracownik, który w ramach wykonywanych zadań przetwarza dane osoby wnioskującej zobowiązany jest dokonać weryfikacji przetwarzanych danych.

W przypadku stwierdzenia konieczności wprowadzenia zmian informuje o tym bezpośredniego przełożonego. Następnie niezwłocznie dokonuje zmian, rejestrując ten fakt w aktach sprawy. Uzupełnienie danych następuje zawsze z uwzględnieniem celów przetwarzania.

Prawo do sprostowania danych w trybie art. 16 RODO nie znajdzie zastosowania do danych osobowych, w odniesieniu do których tryb ich sprostowania lub uzupełnienia określają odrębne przepisy, np. procedura sprostowania błędów i omyłek zawartych w decyzji administracyjnej w trybie art. 113 KPA

- **w przypadku prawa do usunięcia danych („prawo do bycia zapomnianym")** (art. 17 RODO) – osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
  a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób są przetwarzane,
  b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zarówno danych zwykłych jak i szczególnych kategorii danych, a jednocześnie nie ma innej podstawy prawnej ich przetwarzania,
  c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
  d) dane osobowe były przetwarzane niezgodnie z prawem,
  e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.

Prawo do usunięcia danych, co do zasady nie będzie mogło być zrealizowane przez Szkołę/Przedszkole **z uwagi na fakt, że w większości przypadków podstawą prawną ich przetwarzania są przepisy prawa, z których wynika m.in. obowiązek przechowywania dokumentacji (archiwizacji) przez okres wynikający z Jednolitego Rzeczowego Wykazu Akt.**

- **w przypadku prawa do ograniczenia przetwarzania** (art. 18 RODO) polega na tym, że osoba, której dane dotyczą ma prawo żądania od administratora ograniczenia przetwarzania danych, w przypadkach określonych w art. 18 ust. 1 RODO. Prawo to polega na konieczności ograniczenia przetwarzania danych osobowych wyłącznie do ich przechowywania.
  Inne formy przetwarzania mogą mieć miejsce wyłącznie za zgodą osoby, której dane dotyczą, lub 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 Unii lub państwa członkowskiego.

Ograniczenia przetwarzania dokonuje się poprzez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej, tak aby każda osoba, która jest upoważniona do przetwarzania tych danych była świadoma iż dane te można jedynie przechowywać.

- **w przypadku obowiązku powiadomienia o sprostowaniu, usunięciu danych osobowych lub o ograniczeniu przetwarzania** (art. 19 RODO) - po dokonaniu sprostowania, usunięcia danych osobowych lub ograniczenia przetwarzania informuje się o tym każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Jeżeli osoba, której dane dotyczą zażąda informacji o odbiorcach – Szkoła/Przedszkole wypełnia ten obowiązek.
- **w przypadku prawa do przenoszenia danych** (art. 20 RODO) - przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy, której stroną jest osoba, której dane dotyczą oraz przetwarzanie odbywa się w sposób zautomatyzowany (nie obejmuje danych przetwarzanych w postaci papierowej) – osoba, której dane dotyczą ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące. Dotyczy to danych, które osoba składająca żądanie wcześniej dostarczyła.

Szkoła/Przedszkole wykonując prawo do przenoszenia danych na żądanie osoby, której dane dotyczą (prawo żądania przesłania tych danych osobowych innemu administratorowi), jeżeli jest to technicznie możliwe.

Realizacja tego prawa będzie ograniczona do nielicznych przypadków, z uwagi na podstawy prawne przetwarzania danych osobowych u Administratora Danych, czyli głównie przetwarzanie niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, które nie daje osobie, której dane dotyczą możliwości do skorzystania z prawa do przenoszenia danych.

- **w przypadku prawa do sprzeciwu** (art. 21 RODO) osoba, której dane dotyczą, ma prawo wniesienia w dowolnym monecie sprzeciwu wobec przetwarzania jej danych osobowych. W Szkole/Przedszkolu prawo to będzie realizowane w nielicznych sytuacjach z uwagi na okoliczności uprawniające osobę, której dane dotyczą do korzystania z tego prawa, tj. wynikające z art. 21 ust. 1 i 2 RODO, skutkiem wniesienia sprzeciwu jest zakaz dalszego przetwarzania danych osobowych, chyba że administrator wykaże, że istnieją ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osób, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
- **w przypadku zautomatyzowania przetwarzania danych, w tym profilowania** (art. 22 RODO) – podczas realizacji obowiązków informacyjnych wynikających z art. 13 i art. 14 RODO pracownicy Szkoły/Przedszkola zobligowani są do przekazania informacji o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu oraz o zasadach ich podejmowania, znaczeniu i konsekwencjach dla osoby, której dane dotyczą, jeżeli takie przetwarzanie ma miejsce.
- **w przypadku prawa do bycia poinformowanym o naruszeniu ochrony danych osobowych (art. 34 RODO)** – prawo to jest realizowane z inicjatywy Szkoły/Przedszkola w sytuacji, gdy doszło do naruszenia ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Szkoła/Przedszkole przekazuje osobie, których dane dotyczą informacje wskazane w art. 34 ust. 2 RODO. Zawiadomienie o naruszeniu ochrony danych osobowych, co najmniej zwiera:
  - ✓ informacje opisujące charakter naruszenia ochrony danych osobowych,

- ✓ imię i nazwisko oraz dane kontaktowe inspektora ochrony danych,
- ✓ opis możliwych konsekwencji naruszenia ochrony danych osobowych,
- ✓ opis środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Art. 34 ust. 3 RODO wskazuje okoliczności, kiedy administrator jest zwolniony z zawiadamiania o naruszeniu ochrony danych osobowych.

Szczegółowe zasady dotyczące reagowania na naruszenia i informowania o nich oraz wyjątki od obowiązku informowania - zawiera procedura zgłaszania naruszeń bezpieczeństwa (opisana w Polityce ochrony danych).

3) W celu zapewnienia realizacji praw osób, których dane dotyczą (wynikających z art. 15-21 RODO) Administrator Danych Osobowych, dopuszcza kanały komunikacji z osobą, której dotyczą dane :
   - ***w sposób tradycyjny*** – osoba, której dane dotyczą składa pismo/wniosek podpisany własnoręcznie, osobiście w Zespole Placówek Oświatowych lub przesyła go za pośrednictwem operatora pocztowego na adres siedziby administratora,
   - ***elektronicznie*** – osoba, której dane dotyczą przesyła wniosek elektronicznie na adres poczty elektronicznej jednostki.

   Jeżeli Administrator Danych Osobowych będzie miał uzasadnione wątpliwości co do tożsamości osoby składającej wniosek z zakresu art. 15 - 21 RODO, może zażądać dodatkowych informacji ułatwiających identyfikację wnioskodawcy.
4) Aby nie dopuścić do naruszenia praw lub wolności danych osobowych, spowodowanej naruszeniem bezpieczeństwa danych osobowych Administrator Danych Osobowych zakazuje, realizacji uprawnień wynikających z art. 15- 21 RODO w rozmowie telefonicznej.
5) Wniosek osoby, której dane dotyczą dot. realizacji praw (opisanych w pkt.1) przekazuje się do Inspektora ochrony danych, który koordynuje jego realizację poprzez przekazanie do właściwych komórek organizacyjnych (określonych regulaminem organizacyjnym) w celu ustalenia, gdzie znajdują się dane osobowe wnioskodawcy oraz uzgadnia sposób załatwienia sprawy.
6) Odpowiedzi na żądanie wynikające z art. 15 - 21 RODO dokonuje się na zasadach i w terminach określonych w art. 12 RODO. Dokumentacja (wniosek i odpowiedź) w sprawie dot. realizacji praw osób, których dane dotyczą przechowywana jest w Sekretariacie Dyrektora.

11. Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych osobowych

1) Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
2) Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia:
   a) stan wiedzy technicznej,
   b) koszt wdrażania,
   c) charakter, zakres, kontekst i cele przetwarzania danych,

d) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.

3) Administrator Danych wdraża takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.
4) W szczególności stosowane środki techniczne i organizacje muszą zapewnić, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób.
5) W pierwszej kolejności, Administrator Danych rozważa, czy cel jakiemu ma służyć projektowane rozwiązane jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.
6) Administrator Danych zapewnia, aby spełnienie warunków wskazanych w pkt 1-5 (tzw. zasady *privacy by design* i *privacy by default*) było odpowiednio udokumentowane np. w formie notatki, maila, raportu z przeprowadzonych testów systemu informatycznego, wydruku z ekranu systemu.
7) Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych, został zawarty w rozdziale pt. „Opis środków organizacyjno - technicznych".

12. Profilowanie danych osobowych

1) Przy profilowaniu Administrator Danych Osobowych obowiązkowo wdraża środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą.
2) O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych, a także na każdy wniosek osoby, której dane dotyczą.
3) Każda osoba, której dane dotyczą, ma prawo wyrażenia sprzeciwu na profilowanie jej danych osobowych, jeżeli uzna, że narusza to jej prawa i wolności.

13. Przetwarzanie szczególnych kategorii danych osobowych

1) Przetwarzanie danych osobowych 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 jest możliwe, jeżeli spełniony jest jeden z poniższych warunków:
   a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach;
   b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora Danych lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii Europejskiej, prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

c) przetwarzanie jest niezbędne do ochrony interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
d) 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;
e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania czynności przez sądy;
g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii Europejskiej 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;
h) 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 Europejskiej lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem ochrony zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ppkt. 2;
i) 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 Europejskiej lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
j) 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 RODO, na podstawie prawa Unii Europejskiej 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;
k) art. 89 ust. 1 RODO stanowi, że przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele. Jeżeli cele te można zrealizować w drodze

dalszego przetwarzania danych, które nie pozwalają albo przestały pozwalać na zidentyfikowanie osoby, której dane dotyczą, cele należy realizować w ten sposób.

2) Dane osobowe, których przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, ucznia, wychowanka szko...ły(przedszkola) diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego mogą być przetwarzane, jeżeli są przetwarzane przez - lub na odpowiedzialność - pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii Europejskiej, prawa państwa członkowskiego, przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę, również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii Europejskiej, prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe.

3) Zgodnie z art. 30a ust.1 -2 Prawa oświatowego nauczyciele oraz inne osoby pełniące funkcje lub wykonujące pracę w podmiotach, o których mowa w art. 30a ust. 1, są obowiązani do **zachowania w poufności** informacji uzyskanych w związku z pełnioną funkcją lub wykonywaną pracą, dotyczących zdrowia, potrzeb rozwojowych i edukacyjnych, możliwości psychofizycznych, seksualności, orientacji seksualnej, pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych uczniów.

14. Obowiązek informacyjny

W celu realizacji obowiązku informacyjnego wskazanego w rozporządzeniu 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 osobowych) – Administrator Danych Osobowych wprowadza zasady:

1) **W przypadku zbierania danych osobowych od osoby, której one dotyczą** (art. 13 RODO) **podczas pozyskiwania danych osobowych** podaje następujące informacje:
   a) swoją tożsamość pełna nazwę oraz adres swojej siedziby,
   b) dane kontaktowe do inspektora ochrony danych osobowych,
   c) cel przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
   d) informację o odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją,
   e) gdy ma to zastosowanie informacje o zamiarze przekazywania danych osobowych do państwa trzeciego,
   f) informacje o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia tego okresu,
   g) informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   h) jeżeli przetwarzanie odbywa się na podstawie art.6 ust.1 lit. a) „osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów" lub art. 9 ust. 2 lit. a) „osoba, której dane dotyczą wyraziła zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach chyba, ze prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której

dane dotyczą, nie może uchylić zakazu, k którym mowa w ust. 1 art. 9 RODO – ADO podaje informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

i) informacje o prawie do wniesienia skargi do organu nadzorczego,
j) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
k) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (o którym mowa w art. 22 ust. 1 i 4 RODO).

2) Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały dotychczas zebrane, wówczas przed rozpoczęciem dalszego ich przetwarzania - informuje osobę, którą dotyczą dane o innym celu przetwarzania oraz udziela jej informacji, o których mowa w pkt. 1.
3) **W przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą** (art. 14 RODO) administrator danych podaje następujące informacje:
   a) swoją tożsamość pełna nazwę oraz adres swojej siedziby,
   b) dane kontaktowe do inspektora ochrony danych osobowych,
   c) cel przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania,
   d) kategorie odnośnych danych osobowych,
   e) informację o odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją,
   f) gdy ma to zastosowanie – informację o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej,
   g) informacje o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia tego okresu,
   h) informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   i) jeżeli przetwarzanie odbywa się na podstawie art.6 ust.1 lit. a) „osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów" lub art. 9 ust. 2 lit. a) „osoba, której dane dotyczą wyraziła zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach chyba, ze prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, k którym mowa w ust. 1 art. 9 RODO – ADO podaje informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   j) informacje o prawie do wniesienia skargi do organu nadzorczego,
   k) źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych,
   l) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (o którym mowa w art. 22 ust. 1 i 4 RODO).
4) Obowiązek poinformowania wymieniony w pkt. 4 powinien być wykonany:

a) najpóźniej w terminie miesiąca, mając na uwadze konkretne okoliczności przetwarzania danych osobowych,
b) jeśli dane osobowe maja być stosowane do komunikacji z osoba, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą,
c) lub jeśli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy pierwszym ich ujawnieniu.

5) W każdym przypadku obowiązkiem pracowników jednostki, w działalności w których są zbierane i przetwarzane dane osobowe jest wypełnienie obowiązku informacyjnego, wynikającego z art. 13 i 14 RODO.
6) W celu wypełnienia obowiązku informacyjnego wskazanego w RODO, Administrator Danych Osobowych zobowiązuje do umieszczenia na stronie internetowej klauzuli informacyjnej wynikającej z art. 13 RODO , pod każdym wnioskiem zbieranym od osoby, której dane dotyczą) oraz w miejscu widocznym w sposób zwyczajowo przyjęty.
7) Administrator danych zobowiązuje pracowników – tam, gdzie jest to możliwe w celu wypełnienia obowiązku informacyjnego zamieszana klauzuli informacyjnej na drukach wniosków rozpoczynających daną sprawę.
8) Podanych wyżej zasad **NIE STOSUJE SIĘ**, jeżeli:
   a) dane są przetwarzane przez Administratora Danych na podstawie przepisów prawa,
   b) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
   c) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badań opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania.

15. Procedura zasady retencji danych

1) Zgodnie z zasadą ograniczonego przechowywania opisaną w art. 5 ust. 1 lit.e) RODO dane osobowe u Administratora są 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.
2) Dane osobowe nożna przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania").
3) Administrator Danych Osobowych w celu właściwego zarządzania danymi osobowymi zobowiązuje wszystkich upoważnionych do określenia okresu przechowywania danych, oszacowania okresu przechowywania danych już w chwili ich pozyskania oraz poinformowania zainteresowanych o przewidywanym okresie przechowywania ich danych. Informacje te należy podać w trakcie wypełniania obowiązku informacyjnego, opisanego w podrozdziale „Obowiązek informacyjny".
4) Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych zobowiązana jest do:
   a) nieużywania powtórnego jednostronnie zadrukowanych dokumentów,

b) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy po zakończeniu dnia pracy.

5) Przetwarzanie danych osobowych przez określony termin retencji wynika z prawnego obowiązku nałożonego na administratora danych osobowych. Podstawą prawną ustalającą okres przechowywania danych osobowych stanowią przepisy kancelaryjno-archiwalne (instrukcji kancelaryjnej, jednolity rzeczowy wykaz akt oraz instrukcja w sprawie organizacji i zakresu działania archiwum zakładowego).
6) Po zakończeniu przetwarzania danych osobowych (przetwarzanych w sposób tradycyjny), dane (informacje) powinny być przygotowane przez pracownika merytorycznego do ich przejęcia do archiwum zakładowego lub przekazania do archiwum państwowego.
7) Dokumentację papierową wytworzona u Administratora Danych archiwizuje się w wyodrębnionym pomieszczeniu, tj. w składnicy akt (Archiwum Zakładowym). Dostęp do pomieszczeń posiadają wyłącznie osoby upoważnione przez Administratora Danych Osobowych (archiwista). Po ustaniu okresu archiwizacyjnego dokonuje się brakowania dokumentacji, na podstawie zgody Archiwum Państwowego.

ROZDZIAŁ IV

BEZPIECZEŃSTWO DANYCH U ADMINISTRATORA DANYCH

1. Procedura gromadzenia, wykorzystania, uzupełniania danych oraz przechowywania danych osobowych

1) Przetwarzanie danych osobowych u Administratora Danych odbywa się w zbiorach danych . Dane osobowe gromadzone są:
   a) metodą klasyczną (papierowa) – w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
   b) w systemach informatycznych,
   c) poza zbiorem danych.
2) Dane osobowe przetwarzane u Administratora Danych mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą (obowiązkowe) oraz dobrowolnego oświadczenia woli, lub z innych źródeł, w granicach dozwolonych przepisami prawa.
3) Dane osobowe przetwarza się przy zachowaniu szczególnej staranności, w ochronie interesów osób, których dane dotyczą oraz przy przestrzeganiu **zasad:**
   a) **legalności** – przetwarzania danych zgodnie z przepisami prawa, który został określony w art. 6, 7, 9 i 10 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; w zasadzie legalności szczególną rolę odgrywa przesłanka zgody osoby, której dane dotyczą.
   b) **celowości** – przetwarzania danych dla zrealizowaniu zgodnych z prawem celów,
   c) **merytorycznej poprawności** – przetwarzania danych prawdziwych, kompletnych i aktualnych,
   d) **adekwatności** – przetwarzania wyłącznie tych danych, które są niezbędne do zrealizowania celu(dane osobowe nie mogą być zbierane na zapas tj. bez wykazania celowości ich pozyskania i niezbędności dla realizacji zadań administratora danych),

e) **ograniczenia czasowego** – przechowywania danych nie dłużej, niż to jest konieczne do osiągnięcia celu (np. po okresie użyteczności należy zbiór przekazać do archiwum zakładowego).

4) Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane.
5) Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
6) W przypadku, gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy o ochronie danych osobowych, albo są zbędne do realizacji celu, dla którego zostały zebrane - Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

2. Procedura ochrony danych osobowych:

a) W celu zapewnienia należytej ochrony przetwarzania danych osobowych u Administratora Danych Osobowych zastosowano środki zabezpieczające powierzone zbiory danych w postaci zabezpieczeń technicznych i organizacyjnych.

b) Administrator Danych Osobowych wprowadza do stosowania przez wszystkich pracowników oraz wszystkie pozostałe osoby, które wykonują u Administratora danych pracę na innej podstawie niż stosunek pracy (w tym stażyści, osoby przyjęte na praktyki zawodowe), a także osoby prowadzące jednoosobowe działalności gospodarcze współpracujące z Administratorem danych – **następujące procedury ochrony danych osobowych :**

Zasada czystego biurka

należy przez to rozumieć metodę podnoszącą poziom bezpieczeństwa, zapobiegającą ujawnieniu lub kradzieży informacji, polegającą na:

1. Przechowywaniu przez pracownika na biurku tylko tych dokumentów, które są niezbędne w danym momencie do wykonania bieżących zadań.
2. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej na klucz szafy.
3. Obowiązki określone w pkt 2 pracownik powinien wykonać również w przypadku gdy poweźmie wiadomość, że musi opuścić stanowisko pracy, np. w sytuacjach nagłych, związanych w szczególności ze stanem zdrowia pracownika lub przedłużającą się nieobecnością w biurze,
4. Po zakończonej pracy pracownik może pozostawić na biurku jedynie telefon oraz materiały biurowe, takie jak np. długopis i zszywacz.
5. Obowiązuje zakaz trzymania na biurku wszelkich produktów spożywczych, których posiadanie grozi rozlaniem płynu.
6. Pracownik zobowiązany jest na bieżąco niszczyć te dokumenty, które przestały mu być potrzebne. Dokumenty powinny być niszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji.

Zasada czystego ekranu

to wylogowanie się z systemu przy opuszczaniu stanowiska komputerowego lub zastosowanie wygaszenia ekranu – polegająca na:

1 Każdorazowe opuszczenie pomieszczenia w godzinach pracy powinno zostać poprzedzone zablokowaniem komputera (włączając wygaszasz ekranu) lub w przypadku dłuższej nieobecności wylogować się z systemu.
2 Każdy komputer musi mieć ustawiony wygaszasz ekranu po podaniu hasła lub wyłączający się automatycznie po określonym czasie bezczynności użytkownika,
3 Przy ponownym uruchomieniu komputera należy się zalogować za pomocą hasła dostępu.

Bezpieczeństwo oraz zasady ochrony danych osobowych w systemach informatycznych

1) Zasoby informatyczne służą do realizacji działań służbowych i nie mogą być wykorzystywane do celów prywatnych.
2) Każdy Użytkownik systemu informatycznego stosowanego u Administratora do przetwarzania danych osobowych jest zobowiązany do zapoznania się z zasadami korzystania z tego systemu.
3) Dostęp do danych osobowych mają tylko zalogowani użytkownicy systemu informatycznego z odpowiednimi uprawnieniami i jednocześnie jest możliwość identyfikacji, który z użytkowników odpowiada za dane edytowane, bądź wprowadzone.
4) System informatyczny zabezpieczony jest przed zniszczeniem danych: urządzeniami zabezpieczającymi system (fizycznie) oraz poprzez regularne sporządzanie kopii bezpieczeństwa, które przechowywane są przez informatyków w wyznaczonym miejscu.
5) Użytkownicy mają tak dobrane uprawnienia żeby ograniczyć do minimum możliwość wypływu informacji oraz ich przekłamania lub zmiany. Do programu komputerowego wprowadza się dane po ich fizycznej autoryzacji przez osoby uprawnione do tego.
6) W przypadku przesyłania, udostępniania lub przekazywania dokumentów zawierających dane osobowe do podmiotów (osób) zewnętrznych poprzez teletransmisję danych, zgodnie z procedurami ochrony danych podczas transmisji – określonymi w instrukcji zarządzania danym systemem teleinformatycznym służącym do przetwarzania danych osobowych.
7) Szczegółowe procedury nadawania uprawnień do systemu informatycznego oraz wymogi bezpieczeństwa oraz zasady ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych określa „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

Bezpieczeństwo danych osobowych w pomieszczeniach oraz zasady ochrony danych osobowych w zbiorach nieinformatycznych

1) Dane osobowe mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych.
2) Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe, sale lekcyjne oraz części pomieszczeń, gdzie Administrator Danych prowadzi działalność.
3) Do pomieszczeń przetwarzania danych osobowych zalicza się:

a) sale lekcyjne ,
b) pomieszczenia biurowe, w których zlokalizowane są stacje robocze,
c) pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe,
d) pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego,
e) pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.

4) Przebywanie wewnątrz obszarów, o których mowa w ust. 3, osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych.
5) Kategorycznie zabrania się pozostawiania w pomieszczeniach bez nadzoru uczniów, klientów oraz innych osób, które nie są upoważnione do przetwarzania danych osobowych danego systemu bądź określonej kategorii danych.
6) Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.
7) Osoby opuszczające puste pomieszczenie, w którym przetwarzane są dane osobowe, zobowiązane są do zamknięcia drzwi na klucz. Zabrania się pozostawiania klucza w drzwiach po ich zewnętrznej stronie, za wyjątkiem sytuacji związanych z ochroną przeciwpożarową.
8) Zabrania się samowolnego dorabiania kluczy oraz ich wynoszenia poza siedzibę Administratora Danych..
9) Zobowiązuje się osoby przetwarzające dane osobowe do zachowania szczególnej ostrożności w trakcie prowadzenia rozmów telefonicznych w celu uniknięcia niekontrolowanego udostępnienia danych osobom do tego nieupoważnionym.
10) W celu ograniczenia dostępu osób nieupoważnionych do zbiorów nieinformatycznych zawierających dane osobowe w postaci papierowej, należy :
    a) przechowywać dokumentacje w metalowych szafach, szafach drewnianych lub biurkach wyposażonych w odpowiednie zamki mechaniczne,
    b) przechowywać klucze służące do zabezpieczeń biurek i szaf w miejscach niedostępnych dla osób nieupoważnionych.(odpowiedzialność za należyte zabezpieczenie kluczy ponoszą pracownicy).
    c) wykonywać wydruki oraz kopie dokumentów zawierających dane osobowe jest jedynie dla potrzeb realizacji zadań służbowych oraz realizować je w ramach kompetencji i zakresu nadanych upoważnień.
11) W przypadku przesyłania, udostępniania lub przekazywania dokumentów zawierających dane osobowe do podmiotów (osób) zewnętrznych - dostarczanie przesyłek do wskazanych adresatów, może odbywać się w zaklejonych kopertach z wykorzystaniem:
    a) listu poleconego za potwierdzeniem odbioru.
    b) posłańca lub wskazanej osoby,
    c) innego bezpiecznego sposobu, określonego wymogami prawa lub zawartą umową, gwarantującego bezpieczeństwo danych osobowych.
12) Dokumentację tradycyjną wytworzoną w jednostce po okresie niezbędnym na zajmowanym stanowisku pracy, określonym przepisami kancelaryjno-archiwalnymi przechowuje się w wyodrębnionym pomieszczeniu, tj. składnicy akt (Archiwum Zakładowym). W pomieszczeniu systematycznie monitoruje się temperaturę i wilgotność. Dostęp do

pomieszczenia archiwum posiadają wyłącznie osoby upoważnione przez Administratora Danych Osobowych. Po ustaniu okresu archiwizacyjnego dokonuje się brakowania dokumentacji, z której sporządza się protokół zniszczenia lub przekazuje się ją do Archiwum Państwowego w Kielcach.

Przetwarzanie danych osobowych poza obszarem przetwarzania (dokumentacja tradycyjna, komputery przenośne, elektroniczne nośniki danych)

1) Dopuszcza się możliwość używania urządzeń przenośnych np. dokumentacji papierowej, komputerów przenośnych i tabletów do wykonywania zadań służbowych związanych z przetwarzaniem danych osobowych.
2) Stosuje się elektroniczne zewnętrzne nośniki danych, takie jak: pendreive, płyty kompaktowe CD/DVD, taśmy magnetyczne, dyski twarde.
3) Urządzenia przenośne podlegają tym samym regułom ochrony jak komputery stacjonarne, ponadto podlegają dodatkowej ochronie prawnej ze względu na traktowanie ich jako przenośna baza danych, a szczególnie :
   a) powinny być zabezpieczone fizycznie przed dostępem osób nieuprawnionych - w trakcie użytkowania, transportu,
   b) zabezpieczone przed kradzieżą (np. transport w specjalnej torbie oraz niepozostawianie w widocznym miejscu w samochodzie),
   c) w trakcie pracy poza terenem kontrolowanym przez ADO (np. w pociągu) należy zadbać, aby przetwarzane informacje nie były dostępne dla osób postronnych.
4) Wynoszenie dokumentacji papierowej, komputerów przenośnych (w tym tabletów) poza obszar przetwarzania danych wymaga uzyskania zgody Administratora Danych lub osoby przez niego upoważnionej.
5) W razie zgubienia lub kradzieży urządzenia przenośnego pracownik zobowiązany jest do natychmiastowego powiadomienia o tym bezpośredniego przełożonego, który powiadamia IOD.
6) Zasady ochrony komputerów przenośnych, na których przetwarzane są dane osobowe, określa „Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych".

3. Szkolenia z zakresu ochrony danych osobowych

1) Wszyscy pracownicy posiadający dostęp do danych osobowych przed przystąpieniem do pracy uczestniczą w szkoleniu dotyczącym obowiązujących przepisów prawa z zakresu ochrony danych osobowych oraz obowiązujących procedur wewnętrznych u Administratora Danych.
2) Tematyka szkoleń jest określona w przygotowanym przez Inspektora Ochrony Danych konspekcie szkoleniowym i obejmuje w szczególności:
   -postanowienia Rozporządzenia oraz przepisy krajowe z zakresu ochrony danych osobowych,
   -zasady i procedury określone w Polityce Ochrony Danych Osobowych,
   -obowiązki osób upoważnionych do przetwarzania danych osobowych,
   -odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych.

Sposób zapoznania pracowników z aktami prawnymi dotyczącymi ochrony danych osobowych

1) Każda osoba przy przyjęciu do pracy zapoznaje się z przepisami w zakresie ochrony danych osobowych, co potwierdza własnoręcznym podpisem na oświadczeniu o poufności, którego wzór stanowi **załącznik nr 5 do Polityki** Podpisane przez pracownika oświadczenie o poufności dołącza się do jego akt osobowych.
2) Osobę zatrudnioną oraz ubiegającą się o zatrudnienie informuje się w formie pisemnej o przetwarzaniu jej danych w związku z zatrudnieniem/zawarciem umowy cywilnoprawnej. Informacja po podpisaniu przez pracownika umieszczana jest w jego aktach osobowych.
3) W przypadku kandydatów starających się o zatrudnienie w jednostce informację o przetwarzaniu danych osobowych na potrzeby rekrutacji umieszcza się w ogłoszeniu o naborze na wolne stanowisko pracy.
4) Po zakończonym naborze zebrane dokumenty aplikacyjne kandydatów starających się o zatrudnienie a którzy nie zostali zatrudnieni podlegają zniszczeniu lub odesłaniu na adres osoby przystępującej do naboru.

4. **Procedura rejestracji, aktualizacji oraz wykreślenia zbiorów danych osobowych**

1) Administrator Danych Osobowych zobowiązuje upoważnionych do zgłaszania zbiorów danych do rejestracji inspektorowi ochrony danych osobowych - przed rozpoczęciem czynności przetwarzania.
2) Administrator Danych Osobowych określa **wzór zgłoszenia zbioru danych osobowych do inspektora ochrony danych, który stanowi załącznik nr 11do Polityki.**
3) Każdą zmianę struktury prowadzonego zbioru i miejscach przetwarzania danych osobowych -najpóźniej w dniu podjęcia czynności przetwarzania. Jeżeli zmiana informacji w zgłoszonym zbiorze dotyczy rozszerzenia zakresu przetwarzanych danych - o dane, o których mowa w art. 9 i 10 RODO (część C wniosku, pkt. 6 i 7 - opis kategorii osób, których dane dotyczą, oraz zakresu przetwarzanych danych) – należy zgłosić zmianę przed przetwarzaniem danych w zbiorze.
4) Tryb określony do zarejestrowania zbioru danych stosuje się odpowiednio w razie konieczności aktualizacji lub wykreślenia zgłoszonego zbioru danych osobowych. Do zgłoszenia zmian/wykreślenia zbioru stosuje się wzór zgłoszenia zbioru określony w pkt.2.
5) Inspektor ochrony danych w uzgodnieniu z informatykiem określa warunki techniczne dotyczące zabezpieczeń danych w systemie informatycznym, o których mowa w części E i F zgłoszenia zbioru danych osobowych do rejestracji.
6) Inspektor ochrony danych prowadzi wykaz zbiorów danych osobowych, który stanowi **załącznik 3** do Polityki.
7) W ramach prowadzonego wykazu IOD wpisuje:
   a) wpisuje zbiór danych,
   b) aktualizuje wpisy w wykazie – w przypadku zmiany informacji objętej wpisem,
   c) wykreśla zbiór danych z wykazu – w przypadku zaprzestania przetwarzania w nim danych osobowych,
   d) oraz udostępnia wykaz do przeglądania w siedzibie administratora.

5. Analiza ryzyka i adekwatności środków bezpieczeństwa

1) Administrator Danych przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator Danych analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.
2) Analiza ryzyka pod względem utraty integralności, dostępności lub poufności informacji jest narzędziem niezbędnym do określenia, czy sposoby zabezpieczenia zgromadzonych i przetwarzanych danych u Administratora są adekwatne do ich wartości i czy odpowiadają obowiązującym wymaganiom.
3) Proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji, odnoszącym się do działalności jednostki, dokonywany jest przez IOD we współpracy osobami odpowiedzialnymi za poszczególne obszary działalności jednostki (właścicielami ryzyka) oraz informatykiem w zakresie systemu informatycznego.
4) Narzędziem wsparcia w tym procesie jest arkusz zarządzania ryzykiem w zakresie bezpieczeństwa danych osobowych zawierający ryzyka zidentyfikowane - przy czym katalog zidentyfikowanych ryzyk jest zbiorem otwartym, który może ulegać zmianom w zależności od warunków funkcjonowania jednostki.
5) Pracownicy, do których przypisano poszczególne ryzyka (właściciele ryzyka), określają prawdopodobieństwo wystąpienia zidentyfikowanych ryzyk oraz ich skutek i wpływ na realizowane zadania z jednoczesnym wskazaniem istniejących mechanizmów kontroli i propozycją reakcji na ryzyko. **Właściciele ryzyka corocznie do 30 kwietnia każdego roku przeprowadzają oszacowanie ryzyka dla określonych procesów (operacji) przetwarzania .**
6) **Informatyk corocznie w terminie do 30 kwietnia każdego roku przeprowadza regularnie analizę ryzyk w obszarze przetwarzania danych osobowych w systemie informatycznym.**
7) Na podstawie otrzymanych wyników szacowania ryzyka ochrony danych osobowych przez poszczególnych właścicieli ryzyk – Inspektor Ochrony Danych dokonuje **w terminie do 30 czerwca każdego roku** szacowania ryzyka ochrony danych osobowych który przedstawia w formie raportu z oceny naruszenia praw i wolności osób fizycznych do zatwierdzenia Administratorowi Danych Osobowych.
8) Zasady analizy ryzyka w ochronie danych osobowych i adekwatności środków bezpieczeństwa, **określa Załącznik nr 12 do Polityki.**

Postępowanie z ryzykiem – decyzja Administratora Danych

Reakcja na ryzyko może obejmować :

1) **działanie polegające na modyfikowaniu ryzyka** – reakcje mające na celu wyeliminowanie danego ryzyka lub uwarunkowań z nim związanych w celu ochrony przed skutkami osób fizycznych,
2) **łagodzenie (czyli unikanie) ryzyka** – zmniejszenie prawdopodobieństwa lub skutków niekorzystnego zdarzenia do akceptowalnego poziomu,
3) **przeniesienie** – próba transferu skutków wystąpienia ryzyka na inny pomiot, np. przez wykupienie ubezpieczenia od jakiegoś ubezpieczenia lub scedowanie skutków ryzyka na firmę współpracująca (stosowny zapis w umowie powierzenia).

4) **akceptację** - aktywną (stworzenie planu działania na wypadek wystąpienia ryzyka) lub bierną (niepodejmowanie żadnych działań do momentu wystąpienia ryzyka)

6. **Ocena skutków dla ochrony danych osobowych (*data protection impact assessment*)**

Administrator Danych dokonuje oceny skutków dla ochrony danych w celu opisania przetwarzania danych tam, gdzie zgodnie z analiza ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

7. **Polityka kluczy**

1) Klucze do pomieszczeń, w których przetwarzane są dane osobowe wydawane mogą być wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do tych pomieszczeń na innych zasadach.
2) Administrator Danych Osobowych celem uporządkowania zasad dotyczących zabezpieczenia obiektu (administrowanego budynku), sposobu przechowywania kluczy do pomieszczeń biurowych i gospodarczych oraz dostępu do tych pomieszczeń - wprowadza instrukcję postępowania z kluczami do pomieszczeń oraz sposobu ich zabezpieczenia, która **stanowi załącznik nr 10 do Polityki.**
3) Wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych, w sposób uniemożliwiający dostęp osób trzecich. Osoby postronne mogą przebywać wewnątrz wyżej wymienionego obszaru jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych. W pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu powinny być ustawione w sposób uniemożliwiający wgląd w dane osobom trzecim.
4) Dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (dysk przenośny, pendrive, płyta CD/DVD, karta pamięci) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe - w szafach metalowych lub pancernych. Klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych.
5) W budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do dostępu lub przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem przetwarzania tych danych:
   a) w przypadku, gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe - część, w której są przetwarzane dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej;
   b) wydzielenie części pomieszczenia, w której przetwarza się dane osobowe może być w szczególności realizowane poprzez montaż barierek, lad lub odpowiednie ustawienie mebli biurowych, uniemożliwiające lub co najmniej ograniczające niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.

8. Wydruki

1) Wydruki zawierające dane osobowe, przechowuje się w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce Ochrony Danych Osobowych.
2) Nieprzydatne wydruki papierowe oraz inne dokumenty, zawierające dane osobowe, należy niszczyć w przeznaczonych do tego celu niszczarkach.
3) Za bezpieczeństwo danych osobowych zapisanych w formie papierowej odpowiedzialne są osoby je przetwarzające oraz osoby kierujące pracą działów, pracownicy zatrudnieni na samodzielnych stanowiskach.

ROZDZIAŁ V

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

Przez pojęcie „naruszenia ochrony danych" należy rozumieć „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" (art. 4 pkt 12 RODO).

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych, w tym bezpieczeństwa przetwarzania danych osobowych, na działalność Administratora Danych. Z niniejszej procedury wyłączone są informacje niejawne dla których stosowane są odrębne przepisy.

Opis zdarzeń naruszających ochronę danych osobowych

1) Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) próby naruszenia ochrony danych:
      - z zewnątrz - włamania do systemu, podsłuch, kradzież danych,
      - z wewnątrz - nieumyślna (przypadkowa) lub celowa modyfikacja danych, kradzież danych; wynikająca z przyczyn naturalnych (środowiskowych).
   b) programy destrukcyjne: wirusy, konie trojańskie, makra, bomby logiczne,
   c) awarie sprzętu lub uszkodzenie oprogramowania,
   d) zabór sprzętu lub nośników z ważnymi danymi,
   e) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych,
   f) usiłowanie zakłócenia działania systemu informatycznego;
2) Incydent bezpieczeństwa informacji to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,

c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3) Przyczyną incydentu (zagrożenia) może być:

a) **zdarzenie losowe zewnętrzne** (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może doprowadzić do utraty integralności danych, doprowadzić do ich zniszczenia lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych,

b) **zdarzenie losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy w oprogramowaniu, itp.), które mogą powodować zakłócenia ciągłości pracy systemów, a także prowadzić do zniszczenia lub utraty danych; może nastąpić naruszenie poufności danych.

c) **zamierzone, świadome i celowe** działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych osobowych; jest to najpoważniejsze zdarzenie naruszenia poufności danych, (zazwyczaj nie następuje naruszenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na:

- nieuprawniony dostęp do systemu zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do danych z sieci wewnętrznej,
- nieuprawniony przekaz danych,
- pogorszenie jakości sprzętu i oprogramowania (np. działanie wirusów),
- bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).

d) przyczyna naturalna np. pożar, powódź.

Zagrożenia dla stanowisk komputerowych występują ze względu na ingerencję:

a) SIŁY NATURY - to zdarzenie nie wynikające z działalności człowieka:

- uderzenie pioruna,
- pożar (który jest konsekwencją uderzenia pioruna),
- starzenie się sprzętu komputerowego,
- starzenia się nośników pamięci,
- kurz, smog,
- katastrofy budowlane,
- huragan,
- epidemia,
- ekstremalne temperatury, wilgotność.

b) LUDZI – to celowe lub przypadkowe działanie człowieka (pracownika lub osoby z zewnątrz):

- Błędy i pomyłki użytkowników lub administratorów systemu,
- Błędy utrzymania systemu w poufności, integralności i rozliczalności,
- Zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu,
- Zgubienie nośnika zawierającego dane osobowe,
- Niewłaściwe zniszczenie nośnika,
- Nielegalne użycie oprogramowania,

- Choroba ważnych osób i nieuprawnione zastępstwo (epidemia kadry i brak upoważnienia do dostępu),
- Podpalenie obiektu,
- Zalanie wodą,
- Katastrofa budowlana będąca konsekwencja przypadkowego działania człowieka,
- Zakłócenia elektromagnetyczne, radiotechniczne,
- Podłożenie i wybuch bomby, ładunku wybuchowego,
- Użycie broni,
- Zmiany napięcia w sieci,
- Utrata prądu,
- Zbieranie ładunków elektrostatycznych,
- Utrata kluczowych pracowników,
- Niedobór pracowników,
- Defekty oprogramowania,
- Szpiegostwo,
- Plotkarstwo,
- Terroryzm,
- Wandalizm,
- Kradzież,
- Włamanie do systemu,
- Wyłudzenie, fałszowanie dokumentów,
- Podszycie się pod uprawnionego użytkownika,
- Podsłuch,
- Użycie złośliwego oprogramowania,

c) Podatność systemu na zagrożenia może wynikać z :

- Dostępności systemu wynikającego, m.in. z braku ochrony fizycznej budynku klub znacznej liczby personelu, który posiada dostęp do systemu oraz wiedzę jak go obsługiwać,
- Dostępności informacji znajdującej się w systemie za pośrednictwem połączeń zewnętrznych,
- Możliwości celowego wprowadzenia LUK w sprzęcie i oprogramowaniu lub wprowadzeniu wirusów komputerowych,
- Możliwości awarii sprzętu lub oprogramowania ze względu na uszkodzenie, błędy projektowe lub umyślną interwencje,
- Przesyłanie informacji przez niezabezpieczone łącza telekomunikacyjne.

Naruszenie zabezpieczeń systemu informatycznego

1) Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego dane osobowe jest każdy stwierdzony fakt nieusprawiedliwionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   d) nieautoryzowany dostęp do danych,

e) nieautoryzowane modyfikacje lub zniszczenie danych,
f) udostępnienie danych nieautoryzowanym podmiotom,
g) nielegalne ujawnienie danych,
h) pozyskiwanie danych z nielegalnych źródeł.

2) Naruszenie danych może mieć miejsce również w następujących przypadkach:
   a) zmiana danych bez zgody osoby, której dane dotyczą,
   b) wysłanie danych do niewłaściwej osoby (np. poprzez niewłaściwie zaadresowanie poczty elektronicznej),
   c) utrata nośników danych (telefon, laptop, USB, teczki zawierające dane w wersji papierowej),
   d) nieuprawnione udostępnienie danych (np. elektronicznie – przekazywanie danych przez zdalny dostęp, lub np. telefonicznie (rozmówca podaje się za pracownika policji czy urzędu, próbując wyciągnąć informacje),
   e) nieodpowiednie usuwanie danych (np. administrator postanawia pozbyć się starych komputerów. Przed sprzedażą usuwa jedynie pliki na pulpicie i opróżnia kosz ze starych plików. Nie usuwa jednak danych z dysku komputera).

3) Biorąc pod uwagę standardy bezpieczeństwa teleinformatycznego oraz wytyczne w zakresie polityki bezpieczeństwa opublikowane przez Generalnego Inspektora Ochrony Danych Osobowych (obecnie Urząd Ochrony Danych Osobowych) podstawowe zagrożenia dla danych osobowych przetwarzanych w systemie informatycznym to:
   a) ***utrata poufności informacji*** - polegającej na zapewnieniu, że informacja jest udostępniona jedynie osobom upoważnionym. W związku z tym zagrożenia w zakresie poufności obejmują:
      - nieuprawniony dostęp do obszarów i pomieszczeń, w których zlokalizowane są zasoby systemu informatycznego służącego do przetwarzania danych osobowych,
      - ujawnienie haseł dostępu do systemu informatycznego,
      - nieuprawnione udostępnienie informacji przez osobę uzyskującą dostęp do danych osobowych systemu informatycznego,
      - nieuprawnione przeniesienie informacji na inny nośnik elektroniczny lub papierowy,
      - utrata nośnika zawierającego dane osobowe,
      - podszycie się pod osobę posiadającą uprawnienia użytkownika systemu informatycznego

   b) ***utrata integralności informacji*** - polegającej na zapewnieniu dokładności i kompletności informacji oraz metod jej przetwarzania. Zagrożenia w zakresie integralności obejmują:
      - brak kontroli nad operacjami wykonywanymi na danych osobowych przez użytkowników systemów informatycznych,
      - nieuprawnione przetwarzanie danych osobowych,
      - nieuprawniony dostęp do danych osobowych,
      - błędy sprzętu i systemu informatycznego

   c) ***utrata dostępności informacji*** - polegającej na zapewnieniu, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba. Zagrożenia w zakresie dostępności obejmują:
      - brak możliwości przetwarzania danych osobowych spowodowany brakiem dostępu do pomieszczeń, w których zainstalowane są zasoby systemu informatycznego,
      - awarię sprzętu lub systemu informatycznego,

- zakłócenia w zasilaniu systemu informatycznego,
- brak dostępu do haseł systemu informatycznego,
- klęskę żywiołową.

d) ***oraz rozliczalność***, to zapewnienie aby czynności wykonywane przez użytkowników systemów informatycznych były rejestrowane w celu uniemożliwienia wyparcia się przez osoby wykonujące czynności na danych osobowych. Zagrożenia w systemie informatycznym obejmują:

- brak kontroli nad czynnościami wykonywanymi w systemie informatycznym służącym do przetwarzania danych osobowych,
- nieaktualne listy osób uprawnionych do przetwarzania danych osobowych w systemie informatycznym,
- brak poufności haseł dostępu do systemu informatycznego,
- brak ochrony fizycznej stanowisk dostępu do danych osobowych,
- braki w dokumentacji eksploatacyjnej systemu, w tym dokumentowania zmian systemu.

Przyczyny incydentów bezpieczeństwa informacji mogą dotyczyć:

1) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową
2) działania szkodliwego oprogramowania;
3) próby omijania systemów zabezpieczeń;
4) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów
5) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
6) zniszczenia lub kradzieży nośników danych;
7) próby wyłudzeń informacji;
8) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
9) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
10) naruszenia zasad obowiązujących u administratora dotyczących bezpieczeństwa informacji, w tym danych osobowych (np. pozostawienie włączonego komputera i / lub nie wylogowanie się po zakończeniu pracy lub podczas przerwy w pracy, pozostawienie niezabezpieczonych dokumentów drukowanych zawierających dane osobowe itp.).

Procedura postępowania w przypadku naruszenia bezpieczeństwa danych osobowych w systemach informatycznych i na nośnikach tradycyjnych (procedura alarmowa)

1) Administrator Danych Osobowych w celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanym z ochroną danych osobowych wprowadza procedurę alarmową. Celem procedury jest skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości.

2) W przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych (przetwarzanych w sposób tradycyjny, jak również za pomocą systemów informatycznych) lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, **każdy pracownik zatrudniony** u administratora jest zobowiązany niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego lub inspektora ochrony danych osobowych.
3) ***W razie awarii systemów komputerowych*** **lub awarii sieci** należy powiadomić informatyka.
4) Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   a) opis naruszenia,
   b) określenie sytuacji i czasu, w jakim je stwierdzono,
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia.
   d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
5) Każda osoba, która zauważy i podejrzewa naruszenie bezpieczeństwa danych do momentu przybycia IOD, lub osoby przez niego upoważnionej powinna:
   a) zabezpieczyć dostęp do pomieszczenia lub urządzenia,
   b) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony,
   c) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony,
   d) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych.
6) W przypadku przyjęcia informacji lub stwierdzenia wystąpienia zagrożenia bezpieczeństwa danych osobowych, Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające, w toku którego:
   a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   b) inicjuje ewentualne działania dyscyplinarne,
   c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
   d) dokumentuje czynności podjęte w prowadzonym postępowaniu poprzez sporządzenie pisemnego raportu uchybienia lub zagrożenia bezpieczeństwa danych osobowych – wzór raportu stanowi **załącznik nr 11 do Polityki**,
   e) podejmuje działania zapobiegawcze.
7) Informatyk jest zobowiązany do informowania Inspektora ochrony danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.
8) W przypadku zagrożeń lub stwierdzenia słabości systemu informatycznego informatyk podejmuje następujące działania:
   a) w przypadku stwierdzenia włamania lub podejrzenia włamania do systemu informatycznego zabezpiecza system i dane w nim zawarte poprzez:
      - zmianę hasła administratora, określa rodzaj i sposób włamania,
      - podejmuje działania w celu uniemożliwienia ponownego włamania tego samego typu,
      - szacuje straty w systemie,
      - przywraca stan systemu sprzed włamania,
   b) w przypadku uszkodzenia sprzętu lub programów z danymi określa: przyczyny uszkodzenia, szacuje straty wynikłe z uszkodzenia, dokonuje naprawy oraz ponownego

zainstalowania danego programu, odtworzenia jego pełnej konfiguracji oraz wczytania danych z ostatniej kopii zapasowej.

c) w przypadku uszkodzenia danych osobowych podejmuje następujące działania: ustala przyczynę uszkodzenia danych, określa wielkość i jakość uszkodzenia danych oraz podejmuje działania w celu odtworzenia danych z ostatniej kopii zapasowej,
d) przedkłada raport Administratorowi Danych Osobowych oraz Inspektorowi Ochrony Danych Osobowych, według wzoru raportu opisanego w pkt. 3. IOD przekazany raport ewidencjonuje w dzienniku incydentów i zagrożeń.

9) Raport zawiera co najmniej:
a) kod formy naruszenia danych osobowych wg załączonego katalogu zagrożeń i incydentów bezpieczeństwa danych osobowych, według **załącznika nr 13 do Polityki.**
b) ustala datę, czas, miejsce wystąpienia naruszenia, jego zakres, przyczyny ujawnienia, skutki, oraz wielkość szkód które zaistniały,
c) zabezpiecza ewentualne dowody winy,
d) ustala osoby odpowiedzialne za naruszenia,
e) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
f) inicjuje działania dyscyplinarne,
g) rekomenduje działania prewencyjne (korekcyjne, korygujące, zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości.

10) Inspektor Ochrony Danych sporządzony raport ewidencjonuje w „Dzienniku incydentów i zagrożeń", którego stanowi **załącznik nr 14 do Polityki.**

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1) W przypadku stwierdzenia w toku prowadzonych czynności wyjaśniających wystąpienia naruszenia ochrony danych osobowych podlegającego notyfikacji do organu nadzorczego, zgodnie z art. 33 RODO, po otrzymaniu stosowanej informacji od IOD, ADO -bez zbędnej zwłoki -w miarę możliwości nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia –zgłasza je organowi nadzorczemu, chyba że mało prawdopodobne jest, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2) Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin konieczne jest dołączenie wyjaśnienia przyczyn opóźnienia.
3) Zgłoszenia Administrator Danych Osobowych dokonuje z wykorzystaniem formularza zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego, którego wzór zamieszczony jest na stronie Urzędu Ochrony Danych Osobowych.

Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

1) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO – poza zgłoszeniem takiego naruszenia do organu nadzorczego – bez zbędnej zwłoki zawiadamia o naruszeniu osobę, której dane dotyczą.
2) Zawiadomienie osoby, której dane dotyczą, jasnym i prostym językiem opisuje:
a) charakter naruszenia;
b) zawiera imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) możliwe konsekwencje naruszenia ochrony danych osobowych;

d) środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3) Zawiadomienie osoby, której dane dotyczą, o którym mowa w pkt. 2, nie jest wymagane jeżeli:
   a) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do danych;
   b) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   c) wymagałoby to niewspółmiernie dużego wysiłku – w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje środek, za pomocą osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

ROZDZIAŁ VI

DOKUMENTACJA DOTYCZĄCA MIEJSCA, SPOSOBU I ZAKRESU PRZETWARZANIA DANYCH OSOBOWYCH

1. Obszar przetwarzania danych osobowych oraz wykaz pomieszczeń, w których przetwarzane są dane osobowe

1) Na obszar przetwarzania danych osobowych składają się wszystkie pomieszczenia, w których administrator danych prowadzi swoją działalność .**Obszar ten** obejmuje budynki, pomieszczenia i części pomieszczeń, w których:
   a) przetwarzane są dane osobowe, tzn. miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje, archiwizuje),
   b) jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji,
   c) a także pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych, stacje komputerowe, serwer i inne urządzenia komputerowe, na których dane osobowe są przetwarzane) .
2) Obszar przetwarzania danych osobowych obejmuje teren **szkoły, przedszkola,** który mieści się w budynku przy ul. Zwycięzców 134
3) Dane osobowe mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych. Do pomieszczeń przetwarzania danych osobowych zalicza się:
   a) sale lekcyjne,
   b) gabinet dyrektora,
   c) pracownię komputerowa
   d) sekretariat,
   e) gabinet pedagoga szkolnego,
   f) bibliotekę,
   g) sale sportową,
   h) pokój nauczycielski

i) pomieszczenia biurowe, w których są wprowadzane dane osobowe,
j) pomieszczenia biurowe, w których są przetwarzane dane osobowe,
k) pomieszczenie, w którym wykonywane są kopie zapasowe,
l) pomieszczenie archiwum (składnicy akt),
m) serwerownia.

4) Obszar przetwarzania danych osobowych został szczegółowo opisany w „Wykazie pomieszczeń, w których przetwarzane są dane osobowe", stanowiącym **Załącznik nr 15 do Polityki**. Wykaz ten zawiera następujące informacje:
a) lokalizację budynku,
b) numer pomieszczenia i jego przeznaczenie,
c) wskazanie poziomu budynku,
d) określenie stanowiska użytkującego dane pomieszczenie,
e) wskazanie liczby osób pracujących w pomieszczeniu: wskazanie stanowisk i liczby osób,
f) określenie zabezpieczenia pomieszczenia.

5) Obszar przetwarzania danych osobowych u Administratora Danych, dzieli się na **trzy strefy bezpieczeństwa:**

Do STREFY I – wchodzą: gabinet dyrektora, sekretariat, gabinet pedagoga szklonego, gabinet logopedy, serwerownia, składnica akt (archiwum zakładowe).

Sekretariat i gabinet dyrektora znajduje się na parterze i każdy jest przystosowany do pracy dla jednej osoby, zajmują je dyrektor oraz sekretarz szkoły, w pokojach tych przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji tj. płyty CD przechowuje się w szafach zamykanych na klucze, które są w posiadaniu dyrektora i sekretarza szkoły. W komputerze znajduje się program SIO – system informacji oświatowej. Program może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
W tej strefie może przebywać tylko: dyrektor, osoba obsługująca sekretariat (gabinet oraz sekretariat); informatyk (w serwerowni); składnica akt (archiwum zakładowe) – sekretarz. W strefie mogą przebywać inne osoby, tylko i wyłącznie w obecności osób powyżej wymienionych.
Gabinet pedagoga szkolnego znajduje się na **I piętrze,** a gabinet logopedy na parterze. W gabinetach tym przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji przechowuje się w szafach zamykanych na klucze, które są w posiadaniu pedagoga i logopedy. Komputery mogą uruchomić tylko pracownicy upoważnieni do ich otwarcia przy użyciu odpowiednich haseł.

Do STREFY II – wchodzą: pokój nauczycielski, biblioteka szkolna, świetlica szkolna, sale dydaktyczne oraz pomieszczenie działu księgowości i magazynu żywnościowego.

Pokój nauczycielski znajduje się na **I piętrze** budynku szkolnego. W pokoju, jak i salach dydaktycznych przetwarzane są dane osobowe wychowanków, uczniów i ich rodziców ręcznie (lub elektronicznie). Komputer może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
Dokumentację papierową przechowuje się podczas zajęć dydaktycznych w szafach z przegródkami w pokoju nauczycielskim i salach lekcyjnych, natomiast po zakończeniu zajęć

dzienniki lekcyjne przechowywane są w sekretariacie placówki, zamykane na klucze w szafie pancernej.
Biblioteka szkolna znajduje się na I piętrze budynku szkoły. W pokoju tym przetwarzane są dane osobowe uczniów ręcznie (lub elektronicznie). Komputer może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
Świetlica szkolna znajduje się na I piętrze budynku szkolnego. W pomieszczeniu przechowuje się dziennik zajęć świetlicy w biurku nauczycielskim, w szufladzie zamykanej na klucz, który posiadają wychowawcy świetlicy.
Pomieszczenie działu księgowości znajduje się na I piętrze budynku szkoły. w pokoju tym przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji przechowuje się w szafach zamykanych na klucze, które są w posiadaniu głównego księgowego. Programy może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.

Do tej strefy danych osobowych mają dostęp wszystkie osoby upoważnione, a osoby postronne mogą w niej przebywać, tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych .

Do STREFY III – zalicza się pomieszczenie ogólnodostępne w budynku – należą do nich korytarze, szatnia.

6) Administrator Danych Osobowych :
   a) w celu ochrony obszaru przetwarzania danych osobowych wprowadził **„Instrukcję postępowania z kluczami do pomieszczeń oraz sposobu ich zabezpieczenia”,** która stanowią **załącznik nr 10** do Polityki.
   b) wskazuje, ze sprzątanie pomieszczeń, w których mowa w pkt.3 odbywa się po godzinach pracy Szkoły/Przedszkola, w godzinach pracy ustalonych Regulaminem Pracy.
   c) Pracownicy przetwarzający dane osobowe w godzinach pracy, określonych w Regulaminie Pracy ponoszą pełna odpowiedzialność za nadzór nad powierzonym im miejscem do przetwarzania danych. Po zakończeniu pracy pracownicy są zobowiązani do zabezpieczenia wszystkich dokumentów zawierających dane osobowe oraz sprawdzenia, czy wszystkie urządzenia są wyłączone.
   d) Po godzinach pracy dostęp do wszystkich pomieszczeń, w których przetwarzane są dane osobowe jest całodobowo nadzorowany przez służbę ochrony.
   e) W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych), jednak wymaga to indywidualnej (pisemnej) zgody Administratora Danych Osobowych.

2. Wykaz zbiorów danych osobowych przetwarzanych u administratora

1) W strukturze jednostki wyodrębnione zostały zbiory danych osobowych, których rejestr wraz ze wskazaniem programów stosowanych do ich przetwarzania oraz opisem struktury zbiorów danych osobowych wskazującym zawartość poszczególnych pól informacyjnych i powiązań między nimi zawiera „Wykaz Zbiorów Danych Osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych”, stanowiący **Załącznik nr 3 do niniejszej Polityki.**

2) Wykaz ten zawiera następujące informacje:
   a) Nazwę zbioru danych,
   b) Określenie formy przetwarzania danych osobowych,
   c) Stosowany przy przetwarzaniu danych systemu/ programu,
   d) Autora programu,
   e) Czy dane przekazywane są poza siedzibę jednostki,
   f) Lokalizację bazy danych (miejsce przetwarzania danych),
   g) Zawartość poszczególnych pól informacyjnych w zbiorze,
   h) Typ danych przetwarzanych w zbiorze,
3) Dokumentację systemów oraz programów zastosowanych do przetwarzania danych osobowych, w tym również licencji oprogramowania przechowuje Dział Organizacyjno-Administracyjny.

3. Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Z uwagi na rodzaj i charakter danych osobowych zawartych w zinwentaryzowanych zbiorach danych osobowych - wyróżnia się **trzy kategorie danych**, przetwarzanych u administratora: dane zwykłe , dane osobowe szczególnie chronione oraz niezidentyfikowane..

Pojęcie danych „osobowych zwykłych" zawarte jest art. 4 RODO, "dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej)

Przyjmuje się, ze identyfikacja osoby fizycznej może odbyć się za pomocą najbardziej podstawowych danych: imienia, nazwiska, adresu zamieszkania lub zameldowania, numeru PESEL, NIP czy numeru telefonu, czy numeru IP. Rozporządzenie RODO nie wymienia ich wprost, jednak ze względu na fakt, że właśnie te informacje najdokładniej określają konkretną osobę i są podawane najczęściej, funkcjonują jako dane osobowe zwykłe. Za takim ich zaklasyfikowaniem przemawia też fakt, że ich zdobycie nie wymaga nadzwyczajnych nakładów czasu, środków ani kosztów (na przykład są zbyt ogólnikowe - zidentyfikowanie na ich podstawie konkretnego człowieka byłoby niezwykle trudne), nie stanowią informacji niejawnych, a sami właściciele podają je przy różnych okazjach stosunkowo często.

Ochrona takich danych osobowych polega na określonych w przepisach ograniczeniach, dotyczących przetwarzania danych i uprawnieniach osoby, której one dotyczą.

Dane osobowe zwykłe służą u Administratora danych do wykonywania nałożonych na niego ustawowych zadań i odnoszą się, np. do zatrudnienia pracowników, uczniów(dzieci) i ich rodziców. Zakres tych danych określony jest ustawami, które służą wykonywaniu zadań, wynikających z obowiązku ciążącym na administratorze.

Wyjaśnienie pojęcia danych **osobowych wrażliwych (sensytywnych)** zostało wyjaśnione – w art. 9 RODO – cyt. „Zabrania się przetwarzania danych osobowych 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. Informacje wymienione w przytoczonym przepisie odnoszą się do innej dziedziny życia niż zwykłe dane osobowe. Ich przetwarzanie mogłoby w znacznym stopniu naruszyć intymność ich właściciela, narazić go na dyskryminację lub ośmieszyć ze względu na sfery życia, których dotyczą. Sama idea wyodrębnienia takiej kategorii danych wywodzi się bezpośrednio z prawa każdego człowieka do prywatności."

Dane te są przetwarzane u administratora danych celem wykonywania nałożonych na niego ustawowych zadań i odnoszą się, np. do zatrudnionych pracowników, którzy przedkładają informacje o stanie zdrowia (Zakładowy Fundusz Świadczeń Socjalnych), informacje o skazaniach lub nałożonej kary ograniczenia wolności (w przypadku skazania pracownika), czy opiniach poradni psychologiczno-pedagogicznej..

Administrator danych osobowych, w tym wypadku zawraca szczególna uwagę, by przetworzenie danych „sensytywnych" nie naruszało interesów osoby, której dotyczą dane. Dyrektor Szkoły/Przedszkola/Żłobka/ Klubu dziecięcego - zobowiązuje podległych mu pracowników do przestrzegania zapisu rozporządzenia RODO w zakresie, zapisów art.9 ust. 2, w zakresie ochrony danych wrażliwych - polegającej na umożliwieniu przetwarzania ich tylko w uzasadnionych przypadkach, wymienionych enumeratywnie w ustawie.

Dane te mogą być przetwarzane u administratora tylko i wyłącznie jeżeli - osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

Dane niezidentyfikowane - do procesów przetwarzania danych niezidentyfikowanych dochodzi w ramach stosowanego monitoringu wizyjnego u administratora, którego reguły działania ustala odrębna instrukcja postępowania. Miejsca objęte monitoringiem wizyjnym Administrator oznacza tabliczką informującą o objęciu terenu czy pomieszczeń monitorowaniem.

Opis struktury zbiorów danych osobowych przetwarzanych u administratora, znajduje się w **załączniku nr 3** do niniejszej Polityki „Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych"

4. Sposób przepływu danych pomiędzy poszczególnymi systemami

1) Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki, winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).
2) Przetwarzanie danych osobowych odbywa się na stacjach roboczych użytkowników przy wykorzystaniu programów, systemów wspomagających .
3) Struktura informatyczna jednostki składa się z sieci wewnętrznej mieszczącej się w pomieszczeniach Szkoły/Przedszkola i jest połączona z siecią zbudowaną w oparciu o łącza dzierżawione w Orange SA.
4) Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną jednostki odbywa się : **drogą teletransmisji** - w relacji jednostka organizacyjna - mieszkańcy, klienci,

przedsiębiorcy, kontrahenci, zakład ubezpieczeń społecznych, urząd skarbowy, banki, Narodowy Fundusz Ochrony Zdrowia, urząd wojewódzki, urząd marszałkowski inne jednostki administracji samorządowej i rządowej.

5) Teletransmisji dokonują upoważnione osoby w ramach wykonywania obowiązków służbowych określonych zakresem czynności, tj. w Systemie Informacji Oświatowej (baza danych SIO ; w programie „Płatnik" (aplikacja ZUS), „Obsługa bankowa" (system bankowy – aplikacja przeznaczona do obsługi bankowej firmy dot. wykonywania przelewów bankowych i międzybankowych.
6) Przepływ informacji prowadzonych w formie elektronicznej, odbywa się dwukierunkowo – pomiędzy aplikacjami, a serwerem – dane znajdujące się na serwerze w bazie danych, są pobierane do odczytu lub edycji, po przetworzeniu są na nim zapisywane.
7) Zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych w systemach informatycznych, są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w tych systemach oraz powiązania pól informacyjnych. Informatyk, jako administrator systemu wykonuje, na podstawie aplikacji zastosowanych do przetwarzania danych osobowych opisy oraz aktualizację struktur zbiorów danych wskazujące zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi.
8) Szczegółowe informacje dotyczące przepływu danych osobowych pomiędzy danymi systemami informatycznymi znajdują się w instrukcjach zarządzania danym systemem.

W Szkole / Przedszkolu ustalono **systemy informatyczne: – zał nr 8 polityki.**

1) **System budżetowo-finansowy OPTIVUM**. Producentem programu jest **VULCAN**, z siedzibą we Wrocławiu (kod pocztowy: 51-116), ul. Wołowska 6.

System ten służy do prowadzenia ksiąg rachunkowych jednostki oraz przetwarzania danych osobowych. i obejmuje moduły: FINANSE, PŁACE, KADRY, KASA, MAGAZYN.

Za ww. system odpowiada Główny Księgowy, Specjalista, Sekretarz i Intendent, którzy go obsługują i sporządzają kopie zapasowe bazy danych po każdym dniu pracy na dysku komputera oraz przed każdą aktualizacją na dysku zewnętrznym.
Systemy służą do prowadzenia księgowości, kadr oraz prowadzenia magazynu i stołówki.
Operacje księgowe polegają na rejestracji poszczególnych kwot z zaznaczeniem; przypis, odpis. Moduł magazyn służy prowadzenia bloku żywieniowego. Moduł kadry służy prowadzenia polityki kadrowej.
System wprowadza kontrolę dostępu poprzez wprowadzenie fizycznych i logicznych środków ograniczenia dostępu poprzez hasło i login.
Zasady korzystania z oprogramowania uregulowano Zarządzeniem 3a/2013 Dyrektora Zespołu Placówek Oświatowych z dnia 11 lutego 2013r. w sprawie: wprowadzenia polityki rachunkowości w jednostce.
Dane osobowe pracowników zatrudnionych w jednostce są importowane z systemu KADRY OPTIVUM do programu Płatnik , a następnie przekazywane w drodze teletransmisji do ZUS.

SJOBESTIA (http://www.budzetjst.pl). Program SJO BeSTi@ służy do poprawy zarządzania finansami jednostki samorządu terytorialnego na poziomie jej jednostek organizacyjnych.

Ma na celu wspomożenie służb finansowych JST i JO JST w realizacji zadań w zakresie: planowania budżetu począwszy od etapu przygotowania projektu budżetu,

- poprzez wszystkie jego zmiany, sporządzania sprawozdań jednostkowych w miesięcznych i kwartalnych
- okresach sprawozdawczych, sporządzania bilansów jednostkowych jednostek budżetowych, zakładów
- budżetowych, gospodarstw pomocniczych, bilansów łącznych jednostek organizacyjnych w podziale na formy prawne prowadzonej działalności, bilansów z wykonania budżetu JST oraz bilansu skonsolidowanego,
- wymiany danych między jednostkami organizacyjnymi a jednostką samorządu terytorialnego.

2) **System teleinformatyczny:**

a)Aplikacja „PŁATNIK", System teleinformatyczny udostępniony przez Zakład Ubezpieczeń Społecznych - wymiana informacji pomiędzy ZPO, a ZUS za pośrednictwem Internetu. System umożliwia: sporządzanie deklaracji rozliczeniowych za pracowników, raportów imiennych, automatyczne przesyłanie danych do ZUS oraz odbierania potwierdzeń przesłania dokumentów. Przekazywanie danych odbywa się w postaci elektronicznej przy użyciu certyfikatu kwalifikowanego użytkownika systemu oraz odpowiadającego mu klucza prywatnego;

b)Sprawozdawczości GUS - Serwer zewnętrzny dostęp do aplikacji przez Internet. System umożliwia wykonanie zadań w zakresie sprawozdawczości drogą elektroniczną. Upoważniony (wyznaczony) pracownik przez Dyrektora – w zakresie obowiązków służbowych.

c)ePEFRON - System teleinformatyczny udostępniony przez PEFRON - wymiana informacji pomiędzy ZPO, a PEFRON za pośrednictwem Internetu. Upoważniony (wyznaczony) pracownik przez Dyrektora.

d) GUS - System elektronicznej sprawozdawczości (serwer zewnętrzny dostęp do aplikacji przez Internet).System umożliwia wykonanie zadań w zakresie sprawozdawczości drogą elektroniczną. Dostęp do danych w systemach jest możliwy po wprowadzeniu prawidłowego identyfikatora i hasła. Upoważniony (wyznaczony) pracownik przez Dyrektora – w zakresie obowiązków służbowych.

3)**System informacji oświatowej** - baza danych SIO stanowi centralny zbiór danych, prowadzony przez ministra właściwego do spraw oświaty i wychowania. Dostęp do systemu posiadają osoby upoważnione przez Administratora Danych, które dokonują teletransmisji danych.

W systemie informacji oświatowej są gromadzone i przetwarzane dane osobowe:

a)dzieci objętych wczesnym wspomaganiem rozwoju w szkołach i placówkach oświatowych, dzieci objętych wychowaniem przedszkolnym w przedszkolach, oddziałach przedszkolnych zorganizowanych w szkołach podstawowych i innych formach wychowania przedszkolnego oraz uczniów, słuchaczy, wychowanków i absolwentów szkół i placówek oświatowych;

b)nauczycieli, wychowawców i innych pracowników pedagogicznych, o których mowa w art. 1 ust. 1 i ust. 2 pkt 1-3 ustawy z dnia 26 stycznia 1982 r. - Karta Nauczyciela;

c)nauczycieli, o których mowa w art. 16 ust. 1 ustawy - Prawo oświatowe;
d)osób niebędących nauczycielami, o których mowa w art. 15 ust. 1-5 oraz art. 62 ust. 2 ustawy - Prawo oświatowe;
e)osób, które wykonują zadania nauczyciela na podstawie umowy cywilnoprawnej.

4) **System bankowości internetowej** - udostępniony przez bank - Program umożliwia:

- pobieranie online wyciągów bankowych,
- transmisję do banku przelewów w postaci elektronicznej,
- dokonywanie analizy wolnych środków na poszczególnych rachunkach bankowych sporządzanie czeków gotówkowych,
- stosowanie systemu identyfikacji - każdorazowy przelew jest opatrzony bezpiecznym podpisem elektronicznym, składanym przez upoważnionego pracownika.

Upoważniony pracownika na podstawie karty kryptograficznej.

5)**System organizacyjny edukacji szkolnej**

System ten służy do organizacji roku szkolnego i obejmuje moduły: ARKUSZ OPTIVUM, SEKRETARIAT OPTIVUM, MOL OPTIVUM.
Moduł wspomaga przygotowanie arkusza organizacyjnego szkoły zatrudniającej nauczycieli oraz umożliwia analizowanie i przetwarzanie zawartych w nim danych. Jest punktem wyjścia dla planowania zajęć i dyżurów. Plan lekcji Optivum oraz planowania i rozliczania zastępstw w programie Zastępstwa Optivum.
Moduł służy do prowadzenia ewidencji uczniów. Gromadzone są dane uczniów niezbędne do odwzorowania podstawowej dokumentacji przebiegu nauczania: ksiąg uczniów, ksiąg ewidencji dzieci podlegających obowiązkowi szkolnemu, arkuszy ocen, rejestrów legitymacji i innych dokumentów.
Pozwala na szybkie opracowywanie posiadanych zbiorów Rejestruje każde wypożyczenie, zwrot, prolongatę oraz prowadzenie kontroli zbiorów (skontrum). Tworzy wszystkie niezbędne okresowe sprawozdania statystyczne z pracy biblioteki. Obsługuje proces ewidencji bezpłatnych podręczników. Pozwala na prowadzenie ewidencji zajęć, dzięki wykorzystaniu tzw. Dziennika biblioteki szkolnej. Zapewnia bieżącą kontrolę stanu zbiorów - zarówno pod kątem ilości jak i wartości.
Dostęp do danych w systemach jest możliwy po wprowadzeniu prawidłowego identyfikatora i hasła.

6)**System poczty elektronicznej**.
System przeznaczony do przesyłania bezpiecznej , służbowej poczty elektronicznej.
Wszyscy pracownicy – po wprowadzeniu prawidłowego identyfikatora i hasła.

5. Rejestr czynności przetwarzania danych oraz podstawy przetwarzania

1) Rejestr czynności przetwarzania danych stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2) Administrator Danych Osobowych prowadzi rejestr czynności przetwarzania danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

3) Rejestr czynności przetwarzania danych jest jednym z podstawowych narzędzi umożliwiających Administratorowi Danych rozliczanie większości obowiązków ochrony danych.
4) W rejestrze, dla każdej czynności przetwarzania danych, którą Administrator Danych Osobowych uznał za odrębną dla potrzeb rejestru, ADO odnotowuje co najmniej:
   a) nazwę czynności,
   b) cel przetwarzania,
   c) opis kategorii osób,
   d) opis kategorii danych,
   e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu ADO jeśli podstawą jest uzasadniony interes,
   f) sposób zbierania danych,
   g) opis kategorii odbiorców danych (w tym przetwarzających),
   h) informację o przekazaniu poza EU/EOG;
5) Wzór rejestru czynności przetwarzania danych **stanowi załącznik nr 7 do Polityki.**
6) Administrator Danych Osobowych dokumentuje w rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
7) Administrator Danych Osobowych 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 (sprzeciw, ograniczenie itp.).
8) Każdy osoba przetwarzająca dane, zatrudniona u Administratora Danych ma obowiązek znać podstawy prawne, na jakich są przetwarzane dane w konkretnych czynnościach ich przetwarzania – w tym zakresie współpracuje z IOD celem aktualizacji rejestru.

ROZDZIAŁ VII

CIĄGŁOŚĆ DZIAŁANIA

1) Do zapewnienia zgodności z art. 32 ust. 1 lit.b) 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), **tj. zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania** – Administrator wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnia stopienia bezpieczeństwa odpowiadający ryzyku, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
2) W celu zminimalizowania ww. ryzyk w działalności statutowej - Administrator Danych przewiduje konieczność zabezpieczenia ciągłości działania dla danych osobowych przetwarzanych:
   a) z wykorzystaniem systemów informatycznych,

b) bez udziału systemów informatycznych

3) Administrator Danych wdraża **plan ciągłości działania** zgodnie, z którym należy postępować w przypadku zaistnienia zdarzeń mających wpływ na bezpieczeństwo informacji oraz ciągłość działania:

Zapewnienie ciągłości dla danych osobowych przetwarzanych z udziałem systemów informatycznych :

Administrator Danych wprowadza się następującą procedurę zgłaszania awarii systemów informatycznych wykorzystywanych do przetwarzania danych osobowych :

1) W przypadku stwierdzenia ***awarii systemów komputerowych*** należy powiadomić Administratora Danych oraz informatyka, obsługującego jednostkę pod względem informatycznym,
2) Czas reakcji i czas naprawy określa umowa pomiędzy Administratorem Danych, a osobą wykonującą naprawy, z zastrzeżeniem, że podjęcie czynności naprawczych nie powinno zostać podjęte później niż 2 godziny od zgłoszenia awarii.
3) Do czasu usunięcia awarii systemu informatycznego, pracownicy jednostki wykorzystują dokumentację papierową, która po usunięciu awarii systemu informatycznego jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu.
4) Wzór dokumentacja papierowej wykorzystywanej alternatywnie w trakcie awarii systemu informatycznego nie musi być ściśle określony. Powinien jednak zawierać elementy niezbędne do kompletnego wprowadzenia danych osobowych do systemu informatycznego. Jeśli dostawca oprogramowania informatycznego przewidział taką sytuację, stosuje się szablony dokumentów papierowych dostarczonych przez dostawcę oprogramowania.
5) Po usunięciu awarii osoba obsługująca podmiot pod względem informatycznym weryfikuje prawidłowość bazy danych, która jest uzupełniana o informacje wytworzone za pomocą zastępczej dokumentacji papierowej.
6) W przypadku uszkodzenia bazy danych należy wykorzystać kopię zapasową w celu przywrócenia poprawności systemu informatycznego.
7) Z czynności mających na celu przywrócenie pracy systemu informatyk sporządza stosowną notatkę.

Zapewnienia ciągłości działania w przypadku braku zasilania elektrycznego w sieci energetycznej (praca na komputerze)

1) Każdy z użytkowników systemu informatycznego, w sytuacji wystąpienia braku zasilania, ma obowiązek:
   a) niezwłocznego, bezpiecznego zakończenia pracy i wyłączenia stacji roboczej (sytuacja ta również dotyczy komputerów przenośnych – kiedy poziom naładowania baterii umożliwia jego pracę bez zasilania, przez co najmniej przez 2 godziny).
   b) zgłoszenia administratorowi braku zasilania sieci.
2) W celu zapewnienia ciągłości działania jeżeli dane osobowe są przetwarzane na komputerach stacjonarnych Administrator Danych zapewnia ich wyposażenie w urządzenia UPS.

Zapewnienie ciągłości pracy sprzętu, na którym przetwarzane są dane osobowe

1) W przypadku awarii urządzenia (stanowiska komputerowego) służącego do przetwarzania danych osobowych – każdy użytkownik stacji roboczej – ma obowiązek zgłoszenia awarii Administratorowi Danych, który powiadamia informatyka obsługującego podmiot pod względem informatycznym.
2) Czas reakcji i czas naprawy określa umowa pomiędzy Administratorem Danych, a osobą wykonującą naprawy, z zastrzeżeniem, że podjęcie czynności naprawczych nie powinno zostać podjęte później niż 2 godziny od zgłoszenia awarii.
3) Do czasu usunięcia awarii, Administrator zapewnia zapasowe urządzenie spełniające wymogi przepisów prawa i umożliwiające realizowanie zadań statutowych.

Zapewnienie ciągłości pracy w przypadku braku dostępu do sieci internetowej

Jeżeli użytkownik stwierdzi brak dostępu do sieci internetowej należy to zgłosić niezwłocznie Administratorowi Danych, który jeśli jest taka potrzeba powiadamia o tym dostawcę usługi oraz ustala termin usunięcia awarii.

Zapewnienie ciągłości pracy systemu przetwarzania danych osobowych bez udziału systemów informatycznych

1) Sytuacjami, które mogą uniemożliwiać przetwarzanie danych osobowych bez wykorzystania systemów informatycznych, czyli użycia dokumentacji papierowej (tradycyjnej) mogą być:
   a) brak możliwości dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
   b) brak możliwości wykorzystania pomieszczeń, w których przetwarzane są dane osobowe ze względu na awarię np. zalanie pomieszczenia, awaria ogrzewania.
2) W przypadku wystąpienia sytuacji, o których mowa w pkt. 1 każdy z użytkowników przetwarzających dane osobowe ma obowiązek zgłoszenia tego faktu Administratorowi Danych oraz Inspektorowi Ochrony Danych,
3) Osoba wyznaczona przez Administratora Danych podejmuje działania dotyczące usunięcia przyczyn opisanych w pkt. 1.
4) W przypadku braku możliwości wykorzystania pomieszczeń do przetwarzania danych osobowych z powodu awarii, Administrator Danych jest zobowiązany wskazać użytkownikowi inne, spełniające wszystkie normy pomieszczenie na terenie jednostki, w którym będzie on mógł kontynuować swoje obowiązki służbowe.

ROZDZIAŁ VIII
OPIS ŚRODKÓW BEZPIECZEŃSTWA - OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH

Wykonując zapis art. 24 ust. 1 i art. 32 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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 osobowych) oraz § 4 pkt.5 rozporządzenia w Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych(Dz. U. z 2004 r. Nr 100, poz. 1024) - Administrator Danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

W **Zespole Placówek Oświatowych** środki bezpieczeństwa ochrony danych niezbędne do zapewnienia poufności, integralności i rozliczalności zostały pogrupowane na trzy kategorie: środki organizacyjne, środki ochrony fizycznej oraz mechanizmy ochrony informatyczno - technicznej.

I. środki organizacyjne:

1) Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania. Osoby upoważnione do przetwarzania danych mają przydzielone minimalne prawa dostępu do przetwarzania danych osobowych w zależności od wymagań ich stanowiska pracy oraz realizowanych zadań.
2) Jest prowadzona: ewidencja wydanych upoważnień do przetwarzania danych oraz wykaz zbiorów przetwarzanych u Administratora.
3) Osoby upoważnione do przetwarzania danych zostały pouczone o obowiązku zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4) Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
5) Wyznaczono inspektora ochrony danych.
6) Osoby upoważnione do przetwarzania danych zostały zapoznane z przepisami o ochronie danych osobowych poprzez szkolenie przeprowadzone przez inspektora ochrony danych.
7) Osoby trzecie przebywają w obszarze przetwarzania danych wyłącznie w obecności osoby upoważnionej. Osoby trzecie mogą w wyjątkowych okolicznościach przebywać w obszarze przetwarzania danych po uprzednim wydaniu na to zgody przez administratora.
8) Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
9) Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.

Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.

10) Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
11) Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta*.
12) Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
13) W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
14) Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
15) Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
16) W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
17) Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.
18) Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).
19) Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.
20) Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.
21) Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.
22) Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.
23) Opracowano i wdrożono dokumentację zapewniająca ochronę bezpieczeństwa danych, tj. Politykę ochrony danych oraz Instrukcję Zarządzania Systemem Informatycznym, które podlegają okresowym przeglądom i aktualizacji.
24) Opracowano i wdrożono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
25) W przypadku przetwarzania danych osobowych na urządzeniach przenośnych lub dokumentach papierowych poza obszarem przetwarzania należy bezwzględnie chronić te dane przed dostępem do nich osób nieupoważnionych. Dokumentacje papierową oraz

komputery przenośne można wynosić poza siedzibę jednostki, tylko po wydaniu zgody przez Administratora Danych Osobowych.

26) Komputery przenośne, wykorzystywane do przetwarzania danych osobowych po zakończonej pracy są przechowywane w warunkach zapewniających ich bezpieczeństwo.

27) Czas przebywania pracowników na terenie siedziby Administratora Danych określony został w Regulaminie Pracy oraz Regulaminie Organizacyjnym jednostki. Pracownicy mogą przebywać na terenie budynku - tylko w godzinach pracy. Przebywanie na terenie budynku poza wyznaczonymi godzinami pracy lub w dni wolne od pracy jest dozwolone za zgodą Dyrektora jednostki - procedury uzyskania zgody regulują ww. dokumenty.

28) Każdy pracownik przed rozpoczęciem pracy podpisuje listę obecności oraz pobiera klucz do pomieszczenia biurowego, w którym wykonuje swoje obowiązki służbowe. Po otwarciu pomieszczeń, przed przystąpieniem do pracy, pracownik sprawdza stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, dokumentacji oraz powierzonego mienia.

29) Wprowadzono obowiązek przestrzegania przez pracowników zasad „czystego biurka", „czystego ekranu" oraz noszenia identyfikatorów, na których znajduje się „imię i nazwisko, stanowisko służbowe".

Ponadto Administrator Danych realizując swoje zadania z zakresu ochrony przetwarzanych danych osobowych Administrator danych dba o :

1) **przetwarzanie powierzonych mu danych - w zgodzie z zasadami, określonymi w art. 5 i 6 Rozporządzenia RODO**, tj.:
   a) zgodności z prawem (legalności), rzetelności i przejrzystości - dane muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
   b) ograniczenia celu przetwarzania danych – dane muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
   c) minimalizacji danych – dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
   d) prawidłowości danych (poprawności) – dane muszą być 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;
   e) ograniczenia przechowywania danych – dane muszą być 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;
   f) zapewnienia bezpieczeństwa danych, w tym integralności i poufności danych – dane muszą być 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.
   g) oraz rozliczarność określoną w art. 5 ust. 2, gdzie będzie musiał Administrator Danych wykazać się z przestrzegania przepisów, raportować ich realizację oraz przedstawiać

dowody świadczące o prawidłowym wykonywaniu obowiązków na wypadek kontroli organu nadzorczego.

2) **przestrzeganie praw osób, których dane dotyczą m.in. poprzez :**

a) podanie w trakcie zbierania danych osobowych informacji : w przepadku zbierania danych osobowych od osoby, której dane dotyczą, określonych art. 13 Rozporządzenia RODO oraz w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą – określonych w art. 14 Rozporządzenia RODO:
- prawie dostępu przysługującego osobie, której dane dotyczą – w zgodzie z art. 15 Rozporządzenia RODO,
- prawie do sprostowania danych osobowych (art. 16 Rozporządzenia RODO),
- prawie powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 Rozporządzenia RODO),
- prawie wniesienia sprzeciwu wobec przetwarzania danych (art.21 Rozporządzenia RODO),
- prawie wniesienia skargi do organu nadzorczego (art. 13 ust2 lit. D Rozporządzenia RODO).

3) **prowadzenie rejestru czynności** przetwarzania danych osobowych (art. 30 Rozporządzenia RODO), oraz udostępnianie go na żądanie organu nadzorczego (art. 30 ust.4 Rozporządzenia RODO).

4) **Współpracę z organem nadzorczym** w ramach wykonywanych zadań (art. 31 Rozporządzenia RODO),

5) Podejmowanie przez Administratora danych odpowiednich działania, w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych oraz zgłasza naruszenie ochrony danych osobowych do organu nadzorczego oraz zawiadamia o tym osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art.33 i 34 Rozporządzenia RODO).

6) Dokonanie oceny sutków planowanych operacji przetwarzania danych przed rozpoczęciem ich przetwarzania (art. 35 Rozporządzenia RODO).

7) Wyznacza inspektora ochrony danych oraz zapewnia mu organizacyjną odrębność (art.37 Rozporządzenia RODO), któremu zapewnia ADO bezpośrednią podległość pod najwyższe kierownictwo.

II. Środki ochrony technicznej

1) Obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych poprzez zastosowanie drzwi z zamkami patentowymi,

2) Dane osobowe w formie papierowej oraz kopie zapasowe danych w formie elektronicznej przechowywane są w zamykanych ognioodpornych, metalowych szafach.

3) Podstawowe zabezpieczenia fizyczne opisane zostały w załączniku do Polityki „Wykaz pomieszczeń, w których przetwarzane są dane osobowe". Podstawowymi środkami ochrony fizycznej danych to zabezpieczenie zbioru danych w pomieszczeniach za pomocą: krat, rolet, drzwi zwykłych (niewzmacnianych i nie przeciwpożarowych), szaf niematalowych lub metalowych, kas pancernych.

4) Pomieszczenia, w których przetwarzane są zbiory danych , zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy.

5) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek do dokumentów lub na postawie umowy zlecenia wyspecjalizowanej firmie.

III. Środki ochrony informatyczno-technicznej

1) Każdy użytkownik ma odrębny identyfikator oraz hasło dostępu.
2) Dostęp do danych w systemie informatycznym jest możliwy wyłącznie po wprowadzeniu identyfikatora oraz udanym uwierzytelnieniu użytkownika.
3) Stosuje się rozwiązania, które polegają na szyfrowaniu danych osobowych przesyłanych przez sieć Internet.
4) Hasła do systemów informatycznych służących do przetwarzania danych osobowych składają się z co najmniej 8 znaków (małe, wielkie litery, przynajmniej jedna cyfra lub znak specjalny); hasła są zmieniane co 30 dni; jeżeli system nie wymusza zmiany hasła, użytkownik jest zobowiązany do zmiany hasła z własnej inicjatywy przed upływem 30 dni.
5) Na komputerach, za pomocą których są przetwarzane dane osobowe, zainstalowano oprogramowanie antywirusowe automatycznie ściągające najnowsze sygnatury wirusów.
6) Dostęp do danych osobowych z sieci publicznej ograniczony jest poprzez zastosowanie sprzętowej zapory ogniowej (Firewall) – chroni ona wszystkie systemy informatyczne przed nieuprawnionym dostępem i atakami z zewnątrz.
7) W razie awarii zasilania komputery podtrzymywane są za pomocą UPS.
8) Zastosowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,
9) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
10) Użytkowanie programów oraz wykorzystywanie zasobów Administratora Danych niezgodnie z zasadami licencji jest zabronione.
11) Stosuje się system ochrony antyspamowej oraz systemy monitorujące działania infrastruktury informatycznej pod kątem wykrywania podatności na włamania.
12) Bieżąca konserwacja sprzętu informatycznego wykorzystanego przez Administratora Danych Osobowych do przetwarzania danych, jest prowadzona tylko przez zatrudnionego informatyka.
13) Administrator Danych Osobowych dopuszcza możliwość konserwacji i naprawy sprzętu poza swoją siedzibą pod warunkiem pozbawienia nośników z danych osobowych i pozostawienia zabezpieczonych nośników w przeznaczonych do tego celu pomieszczeniach.
14) Kopie zapasowe przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
15) Kopie zapasowe są usuwane niezwłocznie po ustaniu ich użyteczności.
16) Niedopuszczalne jest przetwarzanie danych osobowych poza obszarem przetwarzania.
17) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
    a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
    c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

Rozdział IX

POSTANOWIENIA KOŃCOWE

1. Odpowiedzialność służbowa

1) Na pracownikach oraz osobach upoważnionych do przetwarzania danych osobowych, w zakresie ich uprawnień i odpowiedzialności, ciąży obowiązek dbałości o zabezpieczanie danych osobowych przed ich udostępnieniem, zabraniem, przetwarzaniem z naruszeniem ustawy przez osoby nieuprawnione oraz zmianą, uszkodzeniem, utratą lub zniszczeniem.
2) Pracownik, który :
   a) przetwarza dane osobowe do których nie jest upoważniony,
   b) których przetwarzanie jest zabronione,
   c) niezgodne z celem utworzenia zbioru danych lub niezgodnie z zasadami określonymi w art. 6 ust.1 RODO,
   d) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
   e) nie zgłasza IOD zbiorów danych osobowych,
   f) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą o przysługujących jej prawach,
   g) uniemożliwia osobie, których dane dotyczą z korzystania z jej praw podlega odpowiedzialności karnej zgodnie z rozporządzeniem oraz sankcjom określonym w Kodeksie pracy.
3) Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w Polityce ochrony danych osobowych, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe.
4) Łamanie zasad ochrony danych osobowych obowiązujących u Administratora Danych może również zostać uznane za ciężkie naruszenie obowiązków pracowniczych i może skutkować nałożeniem kary porządkowej na zasadach określonych w przepisach prawa pracy.
5) Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu zasad ochrony danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6) Udokumentowane umyślne złamanie zasad określonych w Polityce ochrony danych jest traktowane jako ciężkie naruszenie obowiązków pracowniczych uzasadniające rozwiązanie stosunku pracy bez wypowiedzenia z winy pracownika.
7) Odmowa udzielenia wyjaśnień lub współpracy z Inspektorem Ochrony Danych traktowana będzie jako naruszenie obowiązków pracowniczych.

2. Postanowienia dodatkowe

1) Niniejsza Polityka Ochrony Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2) Niniejszy dokument podlega okresowym przeglądom, realizowanym nie rzadziej niż jeden raz w danym roku kalendarzowym. Za przeprowadzenie przeglądu odpowiedzialny jest Inspektor Ochrony Danych..
3) Polityka ochrony danych przetwarzanych powiązana jest z następującymi dokumentami:

a) „Instrukcją Zarządzania Systemem Informatycznym",
b) Rejestrem czynności przetwarzania danych osobowych u administratora,
c) Zasadami zabezpieczenia obiektu Szkoły/Przedszkola sposobu przechowywania kluczy do pomieszczeń biurowych i gospodarczych oraz dostępu pracowników do tych pomieszczeń,
d) Zasadami analizy ryzyka,
e) Instrukcją monitoringu wizyjnego,
f) Regulaminem pracy,
g) Statutem oraz Regulaminem organizacyjnym jednostki.

4) W sprawach nieuregulowanych niniejszym dokumentem znajdują zastosowanie przepisy 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 z dnia 10 maja 2018 r. o ochronie danych osobowych.(Dz.U. z 2018 r. , poz.1000).

3. Wykaz załączników do Polityki :

Niniejszy dokument zawiera następujące załączniki stanowiące integralną część Polityki ochrony danych osobowych:

1) **Załącznik nr 1** – Wzory wyznaczenia oraz odwołania Inspektora Ochrony Danych,
2) **Załącznik nr 2 -** wzór upoważnienia do przetwarzania danych osobowych,
3) **Załącznik nr 3 -** Wykaz zbiorów danych osobowych, których administratorem jest Zespół Placówek Oświatowych oraz wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
4) **Załącznik nr 4 -** wzór ewidencji osób upoważnionych do przetwarzania danych osobowych,
5) **Załącznik nr 5 -** oświadczenie o poufności danych,
6) **Załącznik nr 6 -** wzór umowy powierzenia, zgodny z art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych),
7) **Załącznik nr 7 -** wzór - rejestru czynności przetwarzania danych,
8) **Załącznik nr 8 -** wzór - wykaz programów, systemów wspomagających funkcjonowanie jednostki,
9) **Załącznik nr 9** rejestru zawierającego wykaz podmiotów, którym powierzono dane,
10) **załącznik nr 10-** instrukcję postępowania z kluczami do pomieszczeń oraz sposobu ich zabezpieczenia.
11) **Załącznik nr 11** - wzór - raport naruszenia bezpieczeństwa danych osobowych (uchybienia lub zagrożenia),
12) **Załączniki nr 12** - Zasady i tryb zarządzania ryzykiem ochrony danych osobowych,
13) **Załącznik nr 13** – katalog zagrożeń i incydentów bezpieczeństwa danych osobowych,
14) **Załącznik nr 14** - wzór – Dziennik incydentów i zagrożeń,
15) **Załącznik nr 15** - wykaz pomieszczeń, w których przetwarzane są dane osobowe.
16) **Załącznik nr 16** - wzór klauzuli informacyjnej dot. przetwarzania danych osobowych pozyskanych od osoby, której dane dotyczą (art. 13 RODO),
17) **Załącznik nr 17** - wzór klauzuli informacyjnej dot. przetwarzania danych w przypadku pozyskania danych w sposób inny niż od osoby, której dane dotyczą (art. 14 RODO),
18) **Załącznik nr 18** - wzór - karta zgłoszenia zbioru danych osobowych do Inspektora Ochrony Danych,
19) **Załącznik nr 19** - wzór uprawnień do przetwarzania danych osobowych w systemie informatycznym,
20) **Załącznik nr 20** – wzór wniosku o wyrażenie zgody poza obszarem przetwarzania danych (dokumentacja tradycyjna oraz sprzęt informatyczny),

Dokument sporządzono:	Pełen podpis Administratora Danych:	Pieczęć
Data: 31/12/ 2019	DYREKTOR mgr Grażyna Wodz	ZESPÓŁ PLACÓWEK OŚWIATOWYCH ul.Zwycięzców 13 26-110 Skarżysko-Kamienna tel./fax (41) 253-23-79 NIP 663-17-37-782 Regon 292424989