Załącznik do Zarządzenia Nr 24/2021
z dnia 28.05.2021r.

POLITYKA
OCHRONY DANYCH OSOBOWYCH
W
SZKOLE PODSTAWOWEJ IM. MARIUSZA ZARUSKIEGO W PUCKU

METRYKA DOKUMENTU

Data	Wersja	Opis	Autor
22.11.2018 r.	1.0	Polityka Bezpieczeństwa Danych Osobowych	
18.05.2021 r.	1.0	Polityka Ochrony Danych	Zespół ds. Ochrony Danych Osobowych
01.02.2022 r.	1.01	Aktualizacja załącznika nr 03 – Wzory poleceń przetwarzania	Zespół ds. Ochrony Danych Osobowych
21.06.2022 r.	1.02	Aktualizacja załączników: zał. 1; zał. 6; zał. 8, zał. 8a	Zespół ds. Ochrony Danych Osobowych
15.02.2023 r.	1.03	Aktualizacja załącznika 13a – wzory obowiązków informacyjnych	Zespół ds. Ochrony Danych Osobowych

Dokument opracował Zespół ds. Ochrony Danych Osobowych w składzie:		
Imię i nazwisko	**Stanowisko**	**Podpis**
Małgorzata Wendt	Inspektor Ochrony Danych do 31.01.2022 r.	
Małgorzata Zgutka	Inspektor Ochrony Danych od 01.02.2022 r.	
Izabela Majkowska	Wicedyrektor	
Katarzyna Drzeżdżon	Sekretarz	
Zdzisław Pruchniewski	Dyrektor / Informatyk	

Zatwierdził Administrator danych		
Imię i nazwisko	**Stanowisko**	**Podpis**
Zdzisław Pruchniewski	Dyrektor	

Spis treści

CZĘŚĆ I

1. WPROWADZENIE

1.1. SKRÓTY I DEFINICJE

Skróty i definicje użyte w niniejszej Polityce ochrony danych osobowych oznaczają:

Skrót lub pojęcie	Definicja
ADO lub Administrator	Administrator Danych Osobowych oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem jest Szkoła Podstawowa w im. Mariusza Zaruskiego w Pucku
ASI	Administrator Systemów Informatycznych – specjalista ds. informatyzacji, wyznaczony przez Dyrektora szkoły do zapewnienia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych oraz prawidłowej eksploatacji sprzętu komputerowego wraz z urządzeniami pomocniczymi i oprogramowaniem
dane osobowe	Wszelkie 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 bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
dane osobowe „wrażliwe" lub szczególne kategorie danych	Szczególnymi przypadkami danych osobowych są szczególne kategorie danych, do których zaliczamy: 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.
Dostępność	Właściwość informacji zapewniająca, że dane są możliwe do wykorzystania przez osoby i podmioty uprawnione na każde żądanie i w określonym czasie.
Integralność	Właściwość informacji zapewniająca, że dane osobowe zostały zmienione lub usunięte przez osobę do tego upoważnioną.
IOD lub Inspektor	Inspektor Ochrony Danych
Naruszenie ochrony danych osobowych	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.

Skrót lub pojęcie	Definicja
Odbiorca	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
Ograniczenie przetwarzania	Oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
Organ nadzorczy	Niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO. Organem nadzorczym w Rzeczypospolitej Polskiej jest Prezes Urzędu Ochrony Danych Osobowych.
Podmiot przetwarzający	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora. Z podmiotem przetwarzającym musi być zawarta specjalna umowa nazywana umową powierzenia danych.
POD	Polityka ochrony danych w Szkole Podstawowej im. Mariusza Zaruskiego w Pucku
Poufność	Właściwość informacji zapewniająca, że dane są udostępniane wyłącznie osobom i podmiotom uprawnionym.
Powierzenie przetwarzania danych	Przetwarzanie danych w imieniu administratora. Powierzenie wiąże się z podpisaniem odrębnej umowy powierzenia danych lub stosownego zapisu w umowie cywilnoprawnej.
Profilowanie	Dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
Przetwarzanie	Operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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.
Pseudonimizacja	Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
Dyrektor	Dyrektor Szkoły Podstawowej im. Mariusza Zaruskiego w Pucku
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 (RODO) z dnia 27 kwietnia 2016 r.

Skrót lub pojęcie	Definicja
Rozliczalność	Właściwość informacji zapewniająca, że działania podmiotu (osoby) mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
System Informatyczny lub SI	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji zastosowanych w celu przetwarzania danych. Na SI składa się cała infrastruktura informatyczna funkcjonująca w Szkole Podstawowej im. Mariusza Zaruskiego w Pucku
Udostępnienie danych osobowych	Ujawnianie danych osobowych podmiotowi lub osobie będącej odbiorcą danych osobowych lub podmiotem/osobą upoważnioną.
Usuwanie danych	Niszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
Zbiór danych	Uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
Zespół ds. Ochrony Danych Osobowych lub ZOD	Zespół powołany odrębnym Zarządzeniem Dyrektora nr z dnia 11.06.2019, w celu skutecznej realizacji zadań Administratora.
Zgoda	Dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

1.2. PODSTAWY PRAWNE POLITYKI

Podstawą prawną niniejszej Polityki ochrony danych (POD) jest art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO), który zobowiązuje Administratora do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Jednym z takich środków organizacyjnych jest niniejsza Polityka ochrony danych.

1.3. CEL POLITYKI OCHRONY DANYCH

1) W celu prawidłowej realizacji zadań Szkoły Podstawowej im. Mariusza Zaruskiego w Pucku będącej Administratorem oraz zapewnienia bezpieczeństwa przetwarzanych danych osobowych, ustanawia się niniejszy dokument jako obowiązujący.

2) Celem wprowadzenia niniejszego dokumentu jest przede wszystkim:

1) zapewnienie:

a) ochrony danych osobowych zarówno w postaci elektronicznej, jak i w postaci dokumentacji papierowej (np. pism i wydruków) przed ich utratą, modyfikacją, zniszczeniem, nadużyciem, nieuprawnionym dostępem, ujawnieniem lub pozyskaniem;

b) bezpiecznego dostępu do informacji i usług świadczonych publicznie przez Administratora podmiotom do tego uprawnionym;

c) ciągłości usług o wymaganym poziomie dostępności;

2) określenie:

a) sposobów zapewnienia bezpieczeństwa danych osobowych, w tym sposobów zabezpieczenia systemu informatycznego;

b) odpowiedzialności związanej z naruszeniem bezpieczeństwa danych osobowych;

c) metod i sposobów postępowania w przypadku naruszenia warunków bezpieczeństwa danych osobowych.

3) uświadomienie potrzeby:

a) ochrony informacji niezależnie od przyjmowanej przez nie formy;

b) przeprowadzenia przeszkolenia z zakresu ochrony danych osobowych.

1.4. ZAKRES OBOWIĄZYWANIA

1) Opisane zasady mają zastosowanie do wszystkich zasobów, w szczególności do:

4) całego systemu informatycznego szkoły - wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych (aplikacji), oraz do dokumentów papierowych, w których przetwarzane są lub będą dane osobowe;

5) informacji będących własnością szkoły lub podmiotów, z którymi jednostka współpracuje, o ile zostały przekazane na podstawie umów powierzania przetwarzania danych osobowych;

6) wszystkich nośników papierowych, magnetycznych, optycznych lub innych, na których są lub będą znajdować się dane osobowe lub inne informacje;

7) wszystkich lokalizacji – filii, budynków i pomieszczeń, w których są lub mogą być przetwarzane dane osobowe.

2) Opisane w POD zasady dotyczą wszystkich bez wyjątku pracowników szkoły, jak również praktykantów, stażystów, wolontariuszy, zleceniobiorców oraz innych osób, których ADO upoważnił do przetwarzania danych osobowych.

1.5. DOSTĘPNOŚĆ I POPULARYZACJA

1) POD została wprowadzona w życie Zarządzeniem Dyrektora, z którym mają obowiązek zapoznać się wszyscy pracownicy.

2) POD wraz z załącznikami dostępna jest w sekretariacie szkoły.

1.6. AKTUALIZACJA POLITYKI OCHRONY DANYCH

POD podlega weryfikacji i aktualizacji każdorazowo w przypadku:

8) zmiany przepisów prawa związanych z POD;

9) zaleceń wynikających z przeprowadzonych audytów bezpieczeństwa;

10) innych znaczących zmian dotyczących sposobu ochrony informacji.

4) Aktualizację POD przygotowuje ZOD, pod kierunkiem Inspektora.

5) Aktualizacja treści załączników nie wymaga wprowadzenia w życie Zarządzeniem Dyrektora.

2. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1) Zasady przetwarzania danych osobowych określone w RODO, stanowią podstawowe wskazówki dla wszystkich, którzy dane osobowe przetwarzają. Stoją one nad procedurami, dlatego mowa jest o nich już na początku Polityki. Zasady przetwarzania danych są ogólne i są niejako „środowiskiem" dla konkretnych procedur.

2) Do przestrzegania poniższych zasad zobowiązani są wszyscy pracownicy szkoły.

2.1. ZASADA RZETELNOŚCI

1) Zasada rzetelności mówi o tym, że dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie oraz w sposób przejrzysty i zrozumiały.

2) Oznacza to:

11) zapewnienie, by przetwarzanie danych zawsze odbywało się w zgodzie z przepisami prawa;

12) dołożenie szczególnej staranności podczas przetwarzania danych w celu ochrony interesów osób, których dane dotyczą;

13) uwzględnienie potrzeb, oczekiwań oraz możliwości percepcji osób przy wykonywaniu obowiązków związanych z przetwarzaniem danych (np. obowiązek informacyjny musi być dostosowany do osoby, wobec której będzie on wykonywany).

2.2. ZASADA CELOWOŚCI

1) Zasada celowości mówi o tym, że zbieranie danych osobowych powinno odbywać się na podstawie jasno określonego, zgodnego z prawem celu, jeśli cel przetwarzania ustanie, musi również ustać samo przetwarzanie danych osobowych. Należy pamiętać, że przechowywanie archiwalne również może być celem przetwarzania.

2) Oznacza to, że:

14) zbierający dane ma obowiązek jasno określić cel przetwarzania danych;

15) cel przetwarzania danych nie może zostać opisany w sposób ogólny;

16) osoba, której dane dotyczą musi zostać poinformowana, w jakim celu będą przetwarzane jej dane osobowe;

17) zbierający dane nie może uzależnić zawarcia umowy od wyrażenia zgody na przetwarzania danych osobowych w innych celach niż cel główny wyrażony w umowie.

2.3. ZASADA ADEKWATNOŚCI

1) Zasada adekwatności mówi o tym, że Administrator danych osobowych powinien przetwarzać tylko te kategorie danych osobowych i tylko o takiej treści, które są niezbędne do osiągnięcia celu przetwarzania danych osobowych.

2) Oznacza to, że Administrator:

a) ma prawo przetwarzać tylko te dane osobowe, dla których wykaże celowość przetwarzania danych;

18) nie może zbierać danych osobowych „na wszelki wypadek" lub „na zapas".

2.4. ZASADA PRAWIDŁOWOŚCI

1) Zasada prawidłowości mówi o tym, że Administrator danych osobowych musi dołożyć wszelkich starań, aby przetwarzane dane osobowe były prawidłowe i aktualne.

2) Oznacza to, że Administrator powinien:

19) każdorazowo, na etapie pozyskiwania danych osobowych, sprawdzać ich wiarygodność (jeśli cel przetwarzania tego wymaga);

20) wdrożyć procedury mające na celu weryfikację danych osobowych oraz postępowanie w przypadku stwierdzenia nieprawidłowości danych osobowych.

2.5. ZASADA OGRANICZENIA PRZECHOWYWANIA

1) Zasada ograniczenia przechowywania mówi o tym, że Administrator jest zobowiązany przechowywać dane osobowe w sposób umożliwiający identyfikację osoby, której dane dotyczą, przez czas nie dłuższy niż jest to wymagane przez cel przetwarzania danych osobowych.

2) Oznacz to, że Administrator:

a) zobowiązany jest przetwarzać dane osobowe tylko do wypełnienia lub ustania celu przetwarzania danych;

b) powinien ustalić termin usuwania danych osobowych, aby zapobiec przechowywaniu danych osobowych przez czas dłuższy aniżeli jest to wymagane;

c) może przechowywać dane osobowe po ustaniu celu ich przetwarzania jedynie dla celów archiwalnych, badań naukowych, badań historycznych lub statystycznych.

2.6. ZASADA POUFNOŚCI

1) Poufność to właściwość informacji, która mówi, że dostęp do danych możliwy jest tylko dla osób upoważnionych, wobec tego zasada poufności mówi, że przetwarzanie danych osobowych powinno być zorganizowane w taki sposób, aby dostęp do tych danych miały jedynie osoby upoważnione, odbiorcy lub podmioty przetwarzające te dane w imieniu Administratora.

2) Oznacz to, że:

21) Administrator jest zobowiązany wdrożyć środki techniczne i organizacyjne mające na celu zapewnić bezpieczeństwo i ochronę danych osobowych;

22) rozliczalność zasady poufności realizować należy przez udokumentowanie, że dane są przetwarzane jedynie przez osoby, którym wydano polecenia do przetwarzania danych lub w innej formie zalegalizowano przetwarzanie danych oraz określenie w jaki sposób zasada poufności

jest realizowana (np. dostęp do zasobów informatycznych dostępny jest tylko za pomocą indywidualnego loginu i hasła).

2.7. ZASADA INTEGRALNOŚCI

1) Zasadę tę realizuje się dzięki przetwarzaniu danych osobowych w taki sposób, że są one integralne, czyli, że nie zmodyfikował ich nikt, kto nie posiadał ku temu uprawnień.

2) Dla realizacji zasady ważne jest zatem, by dane modyfikowane były jedynie przez osoby do tego uprawnione. Zasadę tę realizuje się również dzięki technicznym i organizacyjnym zabezpieczeniom danych.

3) Rozliczalność zasady integralności realizować należy adekwatnie do zasady poufności.

2.8. ZASADA ROZLICZALNOŚCI

Zasada rozliczalności stanowi, że Administrator jest odpowiedzialny za:

a) przestrzeganie zasad przetwarzania danych osobowych wymienionych w niniejszym punkcie Polityki;

b) musi być w stanie wykazać, w jaki sposób te zasady realizuje.

3. PRAWA OSÓB FIZYCZNYCH

1) RODO formułuje szereg praw, które przysługują osobom fizycznym, a których dane przetwarza Administrator. Poniżej krótko opisano każde z nich.

2) Zasady postępowania podczas realizacji niżej wymienionych praw przestawia Instrukcja rozpatrywania żądań osób fizycznych stanowiąca **załącznik nr 2** do niniejszego dokumentu.

3.1. PRAWO DO OCHRONY DANYCH OSOBOWYCH

Prawo do ochrony danych jest pierwszym i najważniejszym prawem jakie RODO daje osobom fizycznym i mówi o tym, że każda osoba, której dane posiada Administrator, ma prawo do tego, by jej dane były przez Administratora oraz personel Administratora chronione.

3.2. PRAWO DO WYRAŻENIA I COFNIĘCIA ZGODY

Każdy ma prawo wyrazić i cofnąć zgodę na przetwarzanie danych. Dotyczy to tych sytuacji, w których nie ma innej przesłanki pozwalającej na przetwarzanie danych.

3.3. PRAWO DO INFORMACJI

1) Prawo do informacji polega na tym, że nakłada na Administratora obowiązek poinformowania osoby fizycznej, od której zbiera on dane osobowe o szeregu faktów dotyczących przetwarzania danych tej osoby – między innymi, kto jest Administratorem, w jakim celu zbierane są dane tej osoby, na jakiej

podstawie prawnej to przetwarzanie się dokonuje, komu dane będą ujawnione, czy jak długo będą przetwarzane. Pełną listę informacji, których Administrator musi udzielić, zawiera art. 13 RODO.

2) Informacji udziela się w sposób pisemny lub w inny np. elektronicznie, możliwie jak najszybciej po, lub najlepiej w czasie zbierania tych danych. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

3) Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, Administrator też zobowiązany jest spełnić obowiązek informacyjny, za wyjątkiem sytuacji, gdy pozyskanie danych wynika z przepisów prawa.

4) Sposób realizacji prawa do informacji wobec kandydatów do pracy, pracowników, praktykantów, stażystów i wolontariuszy opisuje procedura przyjęcia pracownika, zleceniobiorcy, praktykanta, wolontariusza i stażysty zawarta w **załącznikach nr 6 i 13** do niniejszego dokumentu.

5) W zależności od sytuacji niezbędną klauzulę informacyjną pomaga sformułować IOD.

3.4. PRAWO DO DOSTĘPU DO DANYCH

Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

23) jakie są cele przetwarzania;

24) jakie kategorie danych osobowych zbiera Administrator;

25) jakim odbiorcom (lub jakiej ich kategorii), dane osobowe zostały lub zostaną ujawnione, w szczególności odbiorcom z państw trzecich lub organizacji międzynarodowych;

26) jaki jest planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, jakie są kryteria ustalania tego okresu;

27) informacje o prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

28) informacje o prawie wniesienia skargi do organu nadzorczego;

29) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

30) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

31) jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

3.5. PRAWO DO SPROSTOWANIA DANYCH

1) Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

2) Ww. żądanie musi niezwłocznie trafić do komórki organizacyjnej, która będzie właściwa do sprostowania lub uzupełnienia danych.

3) Po sprostowaniu lub uzupełnieniu danych należy niezwłocznie powiadomić o tym osobą, która żądała sprostowania lub uzupełnienia danych.

3.6. PRAWO DO ŻĄDANIA USUNIĘCIA DANYCH

1) 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:

32) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

33) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

34) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;

35) dane osobowe były przetwarzane niezgodnie z prawem;

36) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator;

37) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego dziecku.

2) Jeżeli Administrator upublicznił dane osobowe ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować Administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by Administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3) Usunięcie danych należy zawsze skonsultować z IOD.

3.7. PRAWO DO OGRANICZENIA PRZETWARZANIA

1) Ograniczenie przetwarzania to specjalne oznaczenie przechowywanych danych osobowych, w celu ograniczenia ich przyszłego przetwarzania.

2) Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania w następujących przypadkach:

38) jeżeli kwestionuje ona prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;

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

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

3) Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, 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.

4) Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, która żądała ograniczenia.

3.8. PRAWO DO POWIADOMIENIA O SPROSTOWANIU, USUNIĘCIU LUB OGRANICZENIU PRZETWARZANIA

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał na podstawie:

1) prawa do sprostowania danych,

2) prawa do usunięcia danych,

3) prawa do ograniczenia przetwarzania

każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagało niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

3.9. PRAWO DO PRZENOSZENIA DANYCH

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi, oraz ma prawo przesłać te dane osobowe innemu Administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe, jeżeli przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy oraz przetwarzanie odbywa się w sposób zautomatyzowany.

3.10. PRAWO DO SPRZECIWU WOBEC PRZETWARZANIA

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, gdy:

1) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi lub

2) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

3.11. PRAWO DO KONTAKTU Z INSPEKTOREM

1) Prawo do kontaktu z IOD polega na tym, że każda osoba, której dane przetwarza Administrator ma prawo do kontaktu z IOD w celu wyjaśnienia wątpliwości związanych z przetwarzaniem.

2) W tym celu Administrator na swojej stronie www publikuje imię, nazwisko i adres email Inspektora ochrony danych.

3.12. PRAWO DO ODSZKODOWANIA ZA SZKODĘ MAJĄTKOWĄ LUB NIEMAJĄTKOWĄ

1) Administrator lub podmiot przetwarzający poniesie odpowiedzialność w przypadku spełnienia następujących przesłanek:

41) poniesienia przez podmiot danych szkody majątkowej lub niemajątkowej;

42) naruszenia przez Administratora lub procesora przepisów rozporządzenia (tj. wystąpienia zdarzenia, w wyniku którego doszło do powstania szkody);

43) zaistnienia związku pomiędzy szkodą a naruszeniem;

44) wystąpienia winy w naruszeniu RODO.

2) Ciężar dowodu wystąpienia naruszenia spoczywa na osobie, której dane dotyczą. Jednak zgodnie z zasadą rozliczalności w praktyce to Administrator będzie musiał udowodnić poprawność przetwarzania danych.

CZĘŚĆ II

4. ZAKRES ZADAŃ I ODPOWIEDZIALNOŚCI

1) Wszystkie osoby mające dostęp do danych osobowych są zobowiązane do przestrzegania postanowień niniejszego dokumentu. Szczególnie odpowiedzialne za ochronę informacji są osoby funkcyjne takie jak: ADO, ASI oraz IOD.

2) Odpowiedzialność **wszystkich osób upoważnionych** do przetwarzania danych polega w szczególności na:

45) ochronie powierzonych informacji;

46) nieudostępnianiu informacji osobom nieuprawnionym;

47) przestrzeganiu wymagań i zaleceń POD;

48) zgłaszaniu do IOD sytuacji związanych z naruszeniem zasad ochrony danych osobowych;

49) zachowaniu w tajemnicy chronionych danych oraz sposobów ich zabezpieczenia, także po ustaniu zatrudnienia;

50) zabezpieczeniu przetwarzanych dokumentów przed dostępem osób nieuprawnionych;

51) zachowaniu w tajemnicy swojego hasła do komputera;

52) przestrzeganiu terminu zmiany hasła co **90** dni;

53) zwracaniu uwagi oraz zgłaszaniu do ASI nietypowego zachowania systemu informatycznego, takiego jak: nieoczekiwane efekty dźwiękowe, nieznane nowe pliki lub katalogi, nagłe zmniejszenie się wolnego miejsca na dysku, niespodziewane komunikaty itp. oraz wypadków wykrycia wirusów komputerowych, które nie dają się usunąć przy pomocy zainstalowanego oprogramowania antywirusowego;

54) zapewnieniu bezpieczeństwa urządzeń przenośnych, jeśli takie znajdują się w posiadaniu pracownika.

3) Szczegółowy zakres zadań i odpowiedzialności znajduje się w **załączniku nr 1** do niniejszej Polityki.

5. CZYNNOŚCI PRZETWARZANIA DANYCH

5.1. REJESTR CZYNNOŚCI PRZETWARZANIA

Czynnością przetwarzania jest zespół powiązanych ze sobą operacji na danych (takich jak zbieranie, utrwalanie, porządkowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, przesłanie, udostępnianie, dopasowywanie, ograniczanie, usuwanie lub niszczenie),

wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.

Zgodnie z art. 30 RODO Administrator prowadzi Rejestr Czynności Przetwarzania (RCP).

RCP stanowi dokładny opis każdego zbioru danych w rozbiciu na czynności, które są wykonywane na danych osobowych zawartych w tym zbiorze. Czynności wyróżnione w RCP dotyczą zawsze konkretnej grupy osób, dlatego też RCP podzielony jest na czynności dotyczące pracowników, klientów, stażystów itd.

7) RCP jest sporządzony w wersji pisemnej, w tym elektronicznej. Jest on przechowywany przez Inspektora oraz uaktualniany przez ZOD każdorazowo w przypadku zmiany czynności przetwarzania lub powstania nowej.

5.2. REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

1) Zgodnie z art. 30 RODO Podmiot przetwarzający prowadzi Rejestr Kategorii Czynności Przetwarzania (RKCP).

2) RKCP stanowi opis kategorii przetwarzań dotyczących danych, które zostały powierzone Administratorowi i w stosunku do nich pełni on funkcję podmiotu przetwarzającego.

3) RKCP jest sporządzony w wersji pisemnej, w tym elektronicznej. Jest on przechowywany przez Inspektora oraz uaktualniany przez ZOD każdorazowo w przypadku zmiany kategorii czynności przetwarzania lub powstania nowej.

6. BEZPIECZEŃSTWO FIZYCZNE PRZETWARZANIA DANYCH

6.1. DOSTĘP DO POMIESZCZEŃ I POSTĘPOWANIE Z KLUCZAMI

1) Po wejściu do budynku, w drodze do swojego pomieszczenia pracy, pracownik zwraca uwagę na otwarte lub wyłamane drzwi lub okna oraz ewentualne awarie techniczne. Po otwarciu drzwi wejściowych do pomieszczenia pracy pracownik sprawdza stan pomieszczenia w taki sposób, aby nie zatrzeć ewentualnych śladów włamania. Z uwagi na fakt, że wyznaczeni pracownicy mają własny klucz bądź komplet kluczy do pomieszczenia, w którym pracuje, pracownicy zobowiązani są do natychmiastowego informowania o każdym przypadku zagubienia lub kradzieży klucza. Niedopełnienie tego obowiązku może powodować konsekwencje służbowe.

2) Przed opuszczeniem pomieszczenia w trakcie pracy, pracownik blokuje dostęp do komputera (⊞ + L) oraz zamyka pomieszczenie na klucz, w przypadku, gdy opuszcza je ostatni.

3) Przed zakończeniem pracy pracownik zabezpiecza dokumenty i wyposażenie oraz wyłącza komputer (w uzasadnionych przypadkach ASI może nakazać pozostawienie pracujących aplikacji i włączonej stacji roboczej). Następnie pracownik sprawdza zabezpieczenie pomieszczeń (zamknięcie okien, drzwi i szaf) oraz zamyka pomieszczenie na klucz.

4) Bieżący komplet kluczy pobierany jest z:
- budynek A: pokoju nauczycielskiego (sale lekcyjne), dyżurki woźnej (sale parter i biblioteka) ;
- budynek B: pokoju nauczycielskiego (sale lekcyjne), dyżurki woźnej (sale zajęć dodatkowych na parterze – bud. B) i z sekretariatu (gabinety i biblioteka na parterze – bud. B);

5) Zapasowy komplet kluczy od pomieszczeń znajduje się w :
sekretariacie szkoły (budynek A i B) i zamknięty jest w specjalnie przystosowanej do tego celu szafce.

6.2. MONITORING WIZYJNY

1) Monitoring wizyjny w budynkach Administratora funkcjonuje w oparciu o przepisy art. 108a ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe.

2) Cele, zakres oraz sposób zastosowania monitoringu ustalony został w Statucie szkoły oraz w odrębnym **Zarządzeniu Dyrektora w sprawie wprowadzenia procedury korzystania z monitoringu wizyjnego**.

6.3. PRZETWARZANIE DANYCH W FORMIE PAPIEROWEJ

6.3.1. Polecenia przetwarzania

1) Każda osoba (pracownik, praktykant, wolontariusz, stażysta) dopuszczony do pracy z danymi osobowymi, musi otrzymać polecenie przetwarzania danych, którego wzór stanowi **załącznik nr 3** do niniejszej Polityki. Polecenie to zawiera również klauzulę informacyjną oraz oświadczenie o zachowaniu danych w tajemnicy, które ww. osoba podpisuje i przekazuje do Sekretarza szkoły.

2) Polecenia przetwarzania danych są rejestrowane w sekretariacie szkoły w *Ewidencji osób upoważnionych do przetwarzania danych osobowych*, której wzór stanowi **załącznik nr 5** do niniejszej Polityki.

6.3.2. Przechowywanie

1) Dane osobowe przechowywane w formie papierowej muszą być zabezpieczone przed dostępem osób do nich nieuprawnionym. Niedozwolone jest więc przechowywanie danych podczas nieobecności osoby uprawnionej do danych w miejscach niezabezpieczonych, czyli w otwartych regałach, na szafach, parapetach czy biurkach.

2) Za dane osobowe przetwarzane w formie papierowej odpowiada osoba, która pracuje z konkretnymi danymi – to ona jest odpowiedzialna za zabezpieczenie ich, podczas swojej nieobecności w miejscu pracy. Administrator odpowiedzialny jest za stworzenie takich warunków, w których zabezpieczenie danych będzie możliwe tj. wyposażenie wymaganej ilości szaf i biurek w zamki.

6.3.3. Wydruki

1) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.

2) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

3) Zabrania się powtórnego używania do sporządzania brudnopisów pism, jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione;

4) Po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę Administratora.

6.4. SPRZĄTANIE POMIESZCZEŃ

1) Naczelną zasadą ochrony informacji jest zapewnienie braku dostępu do nich wszystkim, którzy nie są upoważnieni do zapoznawania się z nimi. Ochrona ta spoczywa na każdej osobie mającej w swoim posiadaniu dokumenty zawierające dane osobowe. Zabezpieczenie danych przechowywanych w postaci papierowej zakłada, że znajdują się one w pomieszczeniu, do którego dostęp mają jedynie osoby upoważnione lub zamknięte są w szafach, biurkach, szafkach oraz innych miejscach wyposażonych w zamek patentowy. Przypadkowe osoby nie mogą mieć dostępu do danych osobowych. Szczególnym przypadkiem jest sprzątanie pomieszczeń.

2) Sprzątanie pomieszczeń szkoły odbywa się zarówno w godzinach jak i po godzinach pracy pracowników. W pierwszym przypadku w czasie sprzątania musi być obecny pracownik upoważniony do dostępu do dokumentów, które znajdują się w pomieszczeniu. Pełni on nadzór nad osobą sprzątającą w kwestii dostępu do danych.

3) W pomieszczeniach, w których sprzątanie odbywa się po godzinach pracy należy bezwzględnie przestrzegać zasady zabezpieczenia dokumentów przed zakończeniem dnia pracy – dokumenty z danymi osobowymi muszą być schowane do biurek lub szaf, a te zamknięte na zamki patentowe. Klucze do nich powinny być ukryte w miejscu niedostępnym dla personelu sprzątającego.

7. BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH

7.1. ŚRODKI OCHRONY INFORMATYCZNEJ

Ogólne środki ochrony informatycznej wszystkich zasobów IT w Szkole Podstawowej im. Mariusza Zaruskiego w Pucku opierają się na następujących zasadach:

1) Lokalna sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla programowego.

2) Systemy informatyczne chronione są przed zagrożeniami poprzez zastosowanie logicznych zabezpieczeń, obejmujących kontrolę przepływu danych oraz działań inicjowanych z sieci publicznej.

3) Systemy informatyczne zabezpieczone są oprogramowaniem antywirusowym, które działa w czasie rzeczywistym na wszystkich komputerach, wykrywając i eliminując oprogramowanie złośliwe.

4) Dostęp do systemu operacyjnego komputera oraz do zasobów informatycznych, w których przetwarza się dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem indywidualnego identyfikatora użytkownika oraz hasła (min. **10** znaków, w tym małe i wielkie litery oraz cyfry lub znaki specjalne), którego zmianę domyślnie wymusza system co **90** dni.

5) Na stanowiskach komputerowych wymuszane jest ponowne logowanie się po **10 minutach** bezczynności komputera.

6) Dane osobowe przetwarzane w systemach informatycznych zabezpieczane są poprzez wykonywanie kopii zapasowych tych danych.

7) Urządzenia, dyski lub inne informatyczne nośniki informacji zawierające dane osobowe przeznaczone do:

55) przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odczytanie;

56) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odzyskanie;

57) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odczytanie albo naprawia się je pod nadzorem osoby upoważnionej;

8) W systemach informatycznych wykorzystuje się tylko legalne oprogramowanie, posiadające ważną licencję i niezbędne do wykonywania zadań ustawowych.

9) Wyłączne prawo w zakresie instalowania i usuwania oprogramowania posiada ASI.

7.2. UPRAWNIENIA DO PRZETWARZANIA DANYCH

1) Podstawą nadania uprawnień jest wniosek przełożonego.

2) Stosowany w szkole schemat uprawnień dostępu do zasobów IT zakłada, iż użytkownicy uzyskują dostęp na z góry zdefiniowanym poziomie w zależności od zakresu obowiązków i powierzonych zadań do wykonania na danym stanowisku.

3) Przełożony użytkownika:

58) wnioskuje o nadanie/odebranie pracownikowi uprawnień do przetwarzania danych w systemach/aplikacjach eksploatowanych w sieci LAN/WAN w związku z wykonywanymi przez niego zadaniami,

59) zgłasza do ASI potrzebę nadania/odebrania uprawnień w systemie informatycznym na wymaganym poziomie. Zgłoszenie powinno zostać przesłane elektronicznie na adres ASI.

4) ASI na podstawie otrzymanego zgłoszenia:

60) rejestruje użytkownika w systemie i nadaje/odbiera mu wymagane uprawnienia,

61) informuje w formie elektronicznej użytkownika oraz jego przełożonego,

5) Użytkownik, po otrzymaniu od ASI informacji o założonym koncie z wymaganymi uprawnieniami:

62) loguje się do systemu/aplikacji w celu sprawdzenia poprawności konta i uprawnień,

63) zaleca się, by przy pierwszym logowaniu się do systemu/aplikacji, użytkownik zmienił nadane mu przez ASI hasło.

6) Powyższe zasady nadawania/odbierania uprawnień dostępu do systemów/aplikacji eksploatowanych w sieci LAN/WAN należy stosować również w przypadku wymaganej zmiany w istniejących uprawnieniach użytkownika.

7.3. METODY UWIERZYTELNIENIA

7.3.1. Zarządzanie hasłami użytkownika w systemie informatycznym

W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się następujące mechanizmy kontroli dostępu do tych danych:

1) ASI informuje użytkownika o nadaniu pierwszego/tymczasowego hasła do systemu.

2) System powinien wymuszać zmianę hasła przy pierwszym logowaniu.

3) Hasło musi się składać z co najmniej **10 znaków**, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

4) Użytkownik systemu zobowiązany jest do zmiany swojego hasła, jeżeli zachodzi choćby podejrzenie jego ujawnienia.

5) Zmiana hasła na nowe musi następować nie rzadziej niż co **90 dni** (od ostatniej zmiany). Za zmianę hasła odpowiedzialny jest każdy użytkownik systemu.

6) Hasła nie mogą być powszechnie używanymi wyrazami słownikowymi. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów bądź innych danych bezpośrednio kojarzących się z użytkownikiem.

7) W przypadku zablokowaniu konta lub zapomnieniu hasła użytkownik zgłasza ten fakt ASI, który nadaje nowe hasło tymczasowe i odblokowuje konto. Użytkownik zobowiązany jest do zmiany tego hasła.

8) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.

7.3.2. Zarządzanie hasłami Administratora Systemów Informatycznych

1) Hasła ASI są to specjalne hasła, które mają bardzo szerokie uprawnienia i pozwalają na wykonanie każdego działania w systemie, z tego względu podlegają szczególnej ochronie.

2) Hasło ASI musi się składać z co najmniej **12 znaków**, zawierać małe i wielkie litery oraz cyfry i znaki specjalne,

3) Hasła do kont administracyjnych są przechowywane w postaci zaszyfrowanej.

4) Dane umożliwiające dostęp do kont administracyjnych są zapisane na druku określonym w **załączniku nr 9** do niniejszej Polityki i przechowywane w kopercie, która znajduje się w szafie pancernej. Dostęp do koperty z hasłami ma Dyrektor szkoły.

5) W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których osoba ta miała dostęp.

7.4. ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY

7.4.1. Rozpoczęcie pracy

1) Aby uruchomić komputer wchodzący w skład systemu informatycznego, podłączony fizycznie do sieci lokalnej, należy go włączyć i zalogować się podając własny identyfikator i hasło dostępu.

2) Jeśli użytkownik wprowadzi 3-krotnie błędne hasło, wówczas jego identyfikator. W celu odblokowania swojego identyfikatora, użytkownik postępuje wg instrukcji obowiązującej przy nadawaniu/odbieraniu uprawnień do systemów informatycznych.

7.4.2. Zawieszenie pracy

1) Każde zawieszenie pracy i odejście od komputera **musi być poprzedzone** zablokowaniem klawiatury komputera kombinacją klawiszy **⊞ + L**. Podczas odblokowania klawiatury należy wpisać hasło.

2) Przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane żadne dane osobowe. Użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem i z ustawionym czasem bezczynności na **10 minut**.

7.4.3. Zakończenie pracy

1) Zakończenie pracy na komputerze i wyłączenie komputera powinno być poprzedzone prawidłowym zamknięciem wszystkich aplikacji uruchomionych na komputerze i wylogowaniem się. Jedynie serwery pracują w systemie ciągłym.

2) Kończąc pracą na komputerze należy pamiętać o następujących czynnościach:

- **1)** zamknąć system/aplikację,
- **2)** zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,
- **3)** sprawdzić, czy elektroniczne nośniki informacji zawierające dane nie zostały pozostawione bez nadzoru.

7.5. TWORZENIE KOPII ZAPASOWYCH

1) Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada wyznaczony ASI.

2) ASI sprawuje nadzór nad wykonywaniem ww. kopii zapasowych oraz weryfikuje ich poprawność. Procedura wykonywania kopii zapasowych określona została w niepublikowanym **załączniku nr 10** do niniejszej Polityki.

7.6. POSTĘPOWANIE Z NOŚNIKAMI INFORMACJI

7.6.1. Nośniki do użytku bieżącego

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać, że:

1) dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego Administratora powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty) lub usunięcie danych programem trwale usuwającym pliki;

2) po ustaniu przydatności danych nośniki tradycyjne oraz elektroniczne, jak również uszkodzone płyty oraz pamięci przenośne, należy utylizować.

7.6.2. Nośniki przeznaczone do likwidacji

1) Nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych.

2) Dokumentuje się fakt zniszczenia nośnika w celu umożliwienia w przyszłości odtworzenia losów informacji.

7.6.3. Nośniki przeznaczone do przekazania i naprawy

Nośniki zawierające dane osobowe i przeznaczone do naprawy, przekazywane są do naprawy tylko w przypadku usunięcia wcześniej zapisu tych danych w sposób uniemożliwiający ich odtworzenie.

7.6.4. Przekazywanie nośników poza siedzibę Administratora

1) Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).

2) Zabrania się wynoszenia poza siedzibę szkoły wymiennych nośników informacji, a w szczególności twardych dysków z zapisanymi danymi osobowymi.

3) W sytuacji przekazywania nośników z danymi osobowymi poza siedzibę szkoły należy stosować następujące zasady bezpieczeństwa:

64) adresat powinien zostać powiadomiony o przesyłce;

65) nadawca powinien sporządzić kopię przesyłanych danych;

66) dane przed wysłaniem powinny zostać zaszyfrowane (dane powinny być spakowane, plik zahasłowany), a hasło podane adresatowi inną drogą (np. smsem);

67) nośnik powinien być umieszczony w bezpiecznej kopercie depozytowej;

68) przesyłkę należy przesyłać za pośrednictwem kuriera;

69) adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.

4) Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że odrębne przepisy nakazują zachować ja na dłużej).

7.7. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

7.7.1. Ochrona antywirusowa

1) W systemie informatycznym zastosowany jest program antywirusowy, który zainstalowany jest na każdym komputerze stacjonarnym i mobilnym (laptopie). Skanuje on pliki zapisane na dysku twardym komputera w czasie rzeczywistym. Programem antywirusowym chroniona jest też poczta elektroniczna.

2) Za ochronę antywirusową odpowiada ASI.

3) Czynności związane z ochroną antywirusową systemu informatycznego wykonuje ASI, wykorzystując w trakcie pracy systemu informatycznego moduły programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby systemu informatycznego.

4) Oprogramowanie antywirusowe na wszystkich stanowiskach komputerowych podłączonych do sieci, a aktualizacja oprogramowania antywirusowego odbywa się w sposób automatyczny dla wszystkich komputerów zainstalowanych w sieci.

5) Instalacja oprogramowania antywirusowego oraz jego aktualizacja na komputerach niepodłączonych do sieci, odbywa się nie rzadziej niż raz na pół roku i jest wykonywana przy zastosowaniu nośników zewnętrznych przez informatyka.

6) Użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego, jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania.

7.7.2. Ochrona styku sieci lokalnej i rozległej (LAN/WAN)

ASI jest odpowiedzialny za aktywowanie i poprawną konfigurację specjalistycznego oprogramowania monitorującego wymianę danych na styku:

1) sieci lokalnej i sieci rozległej (LAN/WAN).

2) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

7.7.3. Ochrona przed awarią zasilania

1) System, w którym przetwarzane są dane osobowe powinien posiadać mechanizmy pozwalające zabezpieczyć je przed ich utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2) Dane osobowe przetwarzane w systemie chroni się stosując dedykowaną dla systemów sieć zasilającą, filtry zabezpieczające przed skutkami spadku napięcia oraz urządzenia podtrzymujące zasilanie do momentu poprawnego zapisania danych i wylogowania się użytkownika z systemu.

3) Dane osobowe przetwarzane z wykorzystaniem serwerów należy zabezpieczać przed zanikiem napięcia wykorzystując centralny UPS.

7.8. PRZEGLĄDY, KONSERWACJE I NAPRAWY

7.8.1. Przegląd i konserwacja sprzętu

1) Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację platformy sprzętowej, na której eksploatowany jest system lub aplikacje. Przeglądy i konserwacje systemu wykonuje na bieżąco ASI w następujących przypadkach:

70) zmiany wersji oprogramowania systemu/aplikacji,

71) zmiany wersji oprogramowania na stanowisku komputerowym użytkownika,

72) zmiany systemu operacyjnego platformy sprzętowej, na której eksploatowany jest system/aplikacja,

73) zmiany systemu operacyjnego na stanowisku komputerowym użytkownika,

74) wykonania zmian w systemie/aplikacji spowodowanych koniecznością naprawy lub modyfikacji systemu.

2) Za prawidłowość przeprowadzenia procesu przeglądu i konserwacji sprzętu odpowiada informatyk dokonujący przeglądu.

7.8.2. Konserwacja systemów i aplikacji

1) Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu/aplikacji potrzeby wprowadzenia zmian pozwalających dostosować funkcjonalność systemu/aplikacji do obsługi bieżących i planowanych potrzeb szkoły.

2) Przed dokonaniem zmian w systemie/aplikacji należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych. Sprawdzenie powinno obejmować m.in.:

a) poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika),

b) poprawność działania funkcjonalności systemu/aplikacji sprawdzonej na różnego typu danych,

c) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty, itp.).

7.8.3. Procedura naprawy sprzętu

1) Bieżące naprawy sprzętu prowadzone są tylko przez pracowników obsługujących systemy informatyczne Administratora.

2) ASI dopuszcza konserwowanie i naprawę sprzętu poza siedzibą Administratora danych jedynie po trwałym usunięciu danych osobowych z nośników.

7.8.4. Niszczenie i utylizacja sprzętu

Przeznaczone do likwidacji urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, pozbawia się wcześniej zapisu tych danych oraz dodatkowo uszkadza się w sposób uniemożliwiający odczyt nośnika.

7.9. ZASADY DOSTĘPU DO INTERNETU

1) Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego sprzętu lub oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.

2) Wymagane zabezpieczenia obejmują:

a) stosowanie zabezpieczeń typu Firewall (np.: sprzętowy, programowy, na serwerze, na stacjach roboczych);

b) stosowanie mechanizmów kontroli dostępu do sieci (np.: IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej, technikę NAT, serwer Proxy);

c) zabezpieczenia sieci bezprzewodowych (np.: uwierzytelnianiem EAP, technologią WPA);

d) stosowanie mechanizmów monitorujących przeglądanie Internetu przez użytkowników, uwzględniających:

- blokowanie stron internetowych określonego typu,
- blokowanie określonych stron internetowych,
- analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

7.10. UŻYTKOWANIE POCZTY ELEKTRONICZNEJ

7.10.1. Procedura przyznania pracownikowi firmowego konta poczty elektronicznej

1) Adres indywidualny firmowej poczty elektronicznej pracownika tworzy się według wzorca wskazanego przez administratora.

2) W przypadku adresów grupowych, czyli innych niż utworzone wg ww. wzorca, obowiązuje akceptacja brzmienia adresu przez ASI.

3) Z adresu indywidualnego firmowej poczty elektronicznej w szczególności obowiązani są korzystać kierownicy komórek organizacyjnych, pracownicy zatrudnieni na stanowiskach samodzielnych i specjalistycznych oraz inni pracownicy wskazani przez przełożonego.

4) Adres firmowej poczty elektronicznej zostaje utworzony na serwerach pocztowych będących własnością pracodawcy.

5) Zabrania się tworzenia i używania adresów firmowej poczty elektronicznej korzystając z innych serwerów/domen niż wyznaczone przez administratora.

6) ASI przekazuje pracownikowi szczegóły dotyczące pierwszego logowania.

7) Pracownik jest zobowiązany do nieujawniania hasła do firmowej poczty elektronicznej osobom trzecim.

7.10.2. Zasady korzystania z firmowej poczty elektronicznej

1) Pracownik ma obowiązek korzystania z firmowej poczty elektronicznej zgodnie z zakresem powierzonych zadań i posiadanych kompetencji.

2) Pracownik jest zobowiązany do korzystania z przyznanego adresu mailowego do prowadzenia wszelkiej korespondencji z przełożonymi, podwładnymi i innymi pracownikami oraz rodzicami i uczniami.

3) Przy korespondencji zewnętrznej pracownik winien pamiętać, że kieruje korespondencję w imieniu pracodawcy, wobec czego jest zobowiązany do stosowania następujących, podstawowych reguł:

a) sprawdzać zawartość skrzynki pocztowej z częstotliwością zapewniającą sprawną i terminową realizację zadań i obowiązków pracownika;

b) bez zbędnej zwłoki reagować na każdy list/przesyłkę od podmiotu zewnętrznego i wewnętrznego;

c) zawsze określać temat korespondencji;

d) załączniki będące dużymi plikami (np. grafika) dodawać do listu tylko za zgodą lub na życzenie odbiorcy;

4) W przypadku przesyłania informacji wrażliwych poza organizację należy wykorzystywać mechanizmy kryptograficzne (np. spakowanie danych z wykorzystaniem hasła za pomocą programów takich jak 7-zip, Winrar, itp.), a hasło przesłać innym kanałem komunikacyjnym (np. sms), w ostateczności w kolejnej wiadomości pocztowej;

5) Użytkownik powinien zwracać szczególną uwagę na poprawność adresu odbiorcy.

6) Zaleca się stosowanie pola UDW (kopii ukrytej) w przypadku przesyłania wiadomości do większej liczby odbiorców zewnętrznych.

7) Podczas korzystania z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabronione jest otwieranie załączników i wiadomości poczty elektronicznej od „niezaufanych" nadawców. Nie należy też otwierać podejrzanych załączników przesłanych przez zaufanego nadawcę. W przypadku wątpliwości użytkownik powinien się skontaktować z ASI.

8) Zabronione jest wykorzystywanie poczty elektronicznej do przesyłania spamu oraz używanie kont służbowych do korespondencji prywatnej.

9) W czasie zaplanowanej nieobecności pracownika (urlop, praca zdalna) pracownik może ustawić automatyczną odpowiedź na przesyłane maile. Tzw. autoresponder powinien informować w jakim czasie pracownik będzie nieobecny i kto go zastępuje, z podaniem imienia, nazwiska, adresu mailowego i/lub telefonu do tej osoby.

10) W czasie niezaplanowanej nieobecności pracownika (zwolnienie lekarskie) lub w innej sytuacji, w której pracownik nie może samodzielnie ustawić autorespondera, odpowiedzialny za to jest ASI, jednak musi on otrzymać informacje, o których mowa w pkt 9) od bezpośredniego przełożonego nieobecnego pracownika.

11) Stosowanie zamiast autoresponderów automatycznych przekierowań poczty jest niedopuszczalne, gdyż wprowadza w błąd nadawcę korespondencji, co do osoby adresata i umożliwia udostępnienie danych osobie nieupoważnionej.

12) Autoresponder powinien być wyłączony po powrocie pracownika z nieobecności tak szybko jak to jest możliwe.

7.10.3. Zakres i uprawnienia kontrolne pracodawcy dotyczące firmowej korespondencji elektronicznej Pracownika

1) E-maile wysyłane z firmowej skrzynki pocztowej stanowią własność pracodawcy i pracodawca może je kontrolować.

2) Z uwagi na konieczność zapewnienia ochrony interesu i bezpieczeństwa szkoły pracodawca zastrzega sobie prawo do wglądu we wszystkie wiadomości pracownika o charakterze służbowym (zarówno w skrzynce odbiorczej, w wiadomościach wysłanych i usuniętych).

3) Kontrola służbowej korespondencji pracowników oraz ich poczty elektronicznej może nastąpić po wcześniejszym uprzedzeniu pracownika.

4) Pracodawca ma prawo również do kontroli przestrzegania przez użytkownika zasad korzystania z firmowej poczty elektronicznej.

7.11. ZASADY KORZYSTANIA Z OPROGRAMOWANIA

1) Jakiekolwiek nieautoryzowane używanie, kopiowanie i rozpowszechnianie oprogramowania komputerowego w szkole jest zabronione.

2) Za zarządzanie licencjami oprogramowania w szkole odpowiada ASI, który odpowiedzialny jest za sporządzenie i aktualizowanie elektronicznej ewidencji oprogramowania. Nie wymaga ewidencjonowania oprogramowanie, które jest darmowe, a jednocześnie jego wykorzystanie jest zgodne z obowiązującymi w tym zakresie przepisami prawa.

3) Częścią dokumentową ewidencji są wszystkie dowody legalności oprogramowania, w szczególności: oryginalne licencje na używanie oprogramowania, faktury zakupu, certyfikaty autentyczności, oryginalne media instalacyjne, pudełka i inne dowody wskazane przez producenta oprogramowania.

4) Instalowanie, zmiany i odinstalowywanie oprogramowania możliwe jest tylko przez ASI. Użytkownicy nie mają odpowiednich uprawnień w systemie, by móc instalować i odinstalowywać oprogramowanie.

7.12. ZASADY PRACY ZDALNEJ ORAZ OCHRONY DANYCH NA URZĄDZENIACH MOBILNYCH

1) Poniższe zasady mają pomóc Administratorowi w bezpiecznej konfiguracji sprzętu użytkowanego poza jego siedzibą, gdyż Administrator jest odpowiedzialny za zapewnienie bezpieczeństwa danych osobowych. Zasady zawarte w niniejszym rozdziale są ZALECANE, a nie obligatoryjnie obowiązujące czy wymagane. Należy je zastosować wszędzie tam, gdzie jest taka możliwość (osobne konto pracownicze na sprzęcie prywatnym, szyfrowanie dysku, VPN itd.) oraz gdy ma to uzasadnienie merytoryczne z perspektywy ochrony danych (niższe wymagania stosujemy, przy realizacji szkoleń online, a wyższe, gdy przetwarzanie danych dotyczy przesyłania danych medycznych). Za każdym razem decyduje o tym Administrator.

2) Zasady bezpieczeństwa pracy zdalnej i ochrony danych na urządzeniach mobilnych, obejmują:

a) Zasady konfiguracji sprzętu do pracy zdalnej;

b) Zasady pracy zdalnej na sprzęcie pracodawcy;

c) Zasady pracy zdalnej na sprzęcie prywatnym;

d) Zasady ochrony danych na urządzeniach mobilnych.

7.12.1. Zasady konfiguracji sprzętu do pracy zdalnej

1) Pracownik powinien mieć utworzone odrębne konto (profil) i przyznane adekwatne dla jego roli uprawnienia (domyślnie jako użytkownicy).

2) Urządzenie powinno:

a) być wyposażone w system antywirusowy;

b) być wyposażone w system szyfrowania danych;

c) mieć włączone wszystkie funkcje bezpieczeństwa (np. hasła, automatyczne blokady ekranu);

d) mieć włączone wszystkie automatyczne aktualizacje dla systemu operacyjnego, aplikacji oraz systemu antywirusowego.

3) Połączenie z serwerami powinno być w odpowiedni sposób szyfrowane. Szyfrowanie powinno być wymuszone.

4) Pracownik powinien mieć zainstalowany program, dzięki któremu może spakować i nadać hasło spakowanemu plikowi przed jego wysyłką do pracodawcy lub innego użytkownika (np. 7-Zip) oraz powinien być przeszkolony z jego obsługi. Hasła do tak zabezpieczonego pliku nie mogą być dystrybułowane tym samym kanałem komunikacyjnym niż plik z danymi (telefon, sms).

5) Pracownik IT powinien przeskanować służbowe urządzenia pracowników pod kątem szkodliwego oprogramowania przed ponownym podłączeniem ich do sieci służbowej.

7.12.2. Zasady pracy zdalnej na sprzęcie pracodawcy

1) Pracownik korzysta z Internetu służbowego (np. hotspot Wifi z telefonu służbowego), a jeśli nie jest to możliwe powinien, zmienić domyślne hasło do domowego routera, tak by odpowiadały ono zasadom bezpieczeństwa ustanowionym w Polityce (domyślnie min. 8 znaków).

2) Do systemów / zasobów służbowych pracownik powinien połączyć się używając VPN.

3) Pracownik, w miarę możliwości, powinien wyznaczyć wybraną część swojego mieszkania do wykonywania pracy zdalnej oraz ograniczyć dostęp do niej osobom postronnym (członkom rodziny, znajomym). Należy pamiętać o zasadzie blokowania komputera, natychmiast, gdy tylko pozostawia się urządzenie bez nadzoru (nawet podczas krótkich przerw).

4) Nie powinno drukować się żadnych dokumentów w miejscu pracy zdalnej.

5) Należy przechowywać wszystkie wytworzone informacje na zdalnych serwerach lub na sprzęcie służbowym.

6) Przesyłanie plików zawierających dane osobowe na serwer lub do innych pracowników, powinno odbywać się w bezpieczny sposób opisany w punkcie 7.12.1.

7) Obowiązuje całkowity zakaz:

a) pożyczania urządzenia, na którym prowadzi się pracę zdalną;

b) korzystanie z prywatnej skrzynki pocztowej w czasie zalogowania się na konto służbowe;

c) korzystania z niezabezpieczonych sieci WiFi (takich, do których dostęp jest możliwy bez podania hasła).

7.12.3. Zasady pracy zdalnej na sprzęcie prywatnym pracownika

1) Praca na sprzęcie prywatnym użytkownika powinna zachodzić jedynie w szczególnych okolicznościach oraz musi być poprzedzona wyraźną zgodą administratora danych. Przetwarzanie danych na sprzęcie prywatnym należy traktować jako ostateczność i uznać za zwiększoną podatność na ryzyko naruszenia ochrony danych.

2) Podczas pracy na sprzęcie prywatnym obowiązują te same zasady, które obowiązują podczas pracy na komputerze służbowym (z wyjątkiem pkt. 2 i 5 w części 7.12.2.) oraz dodatkowo:

3) należy przechowywać wszystkie dane osobowe na zdalnych serwerach. Jeśli nie jest to możliwe, dozwolone jest przechowywanie informacji służbowych na przeznaczonych do tego celu urządzeniach mobilnych (np. laptopie, dysku przenośnym), które jednak muszą być zaszyfrowane;

4) w czasie pracy zdalnej na prywatnym urządzeniu, użytkownik powinien do minimum ograniczyć swoją aktywność na lokalnym koncie administracyjnym;

5) po zakończonej pracy zdalnej i wraz z rozpoczęciem pracy w normalnym trybie, pracownik zobowiązany jest do usunięcia wszystkich służbowych danych osobowych ze swojego dysku prywatnego.

7.12.4. Zasady ochrony danych na służbowych urządzeniach mobilnych

1) Urządzenie mobilne to jakiekolwiek urządzenie przetwarzające dane osobowe i umożliwiające ich wynoszenie z miejsca pracy. Jest to więc zarówno służbowy laptop, jak też telefon komórkowy lub tablet.

2) Użytkownik zobowiązany jest do zachowania ostrożności podczas korzystania z urządzeń mobilnych w miejscach publicznych, salach konferencyjnych i innych niezabezpieczonych obszarach.

3) Należy szczególnie pamiętać o zasadach ostrożności podczas przewożenia lub przenoszenia urządzeń mobilnych:

a) muszą one być przewożone w przeznaczonych do tego torbach lub w miejscach, w których są niewidoczne;

b) nie mogą być pozostawiane w aucie, podczas opuszczania go przez użytkownika (ładowanie smartfonów).

4) W urządzeniach mobilnych, w których jest to możliwe (laptopy), znajduje się konto administracyjne, do którego dostęp posiada ASI i tylko on można instalować oprogramowanie.

5) W służbowych urządzeniach mobilnych zbudowanych na systemach Android, iOS lub innych użytkownicy otrzymują urządzenia z zainstalowanym, niezbędnym zestawem aplikacji.

6) Na użytkowniku spoczywa odpowiedzialność instalacji tylko takiego oprogramowania, które nie spowoduje zagrożenia dla bezpieczeństwa informacji. Jeżeli użytkownik nie jest pewny działania danej aplikacji – nie należy jej instalować.

7) Urządzenia mobilne, które mają taką możliwość, zabezpiecza się programem chroniącym przed szkodliwym oprogramowaniem.

8) Urządzenia mobilne, które mają taką możliwość powinny być zaszyfrowane. Urządzenia te zabezpiecza się przed dostępem do nich. Należy pamiętać, że najbezpieczniejszym zabezpieczeniem są w kolejności: hasło, PIN oraz rozpoznawanie linii papilarnych. Ze względów bezpieczeństwa nie używa się jako sposobów identyfikacji: odblokowywania na podstawie twarzy, narysowanego na ekranie wzoru i innych.

9) Hasło lub PIN do służbowego urządzenia mobilnego powinno zostać zapisane na kartce i umieszczone w zaklejonej kopercie, a następnie schowane w bezpiecznym miejscu zamykanym na klucz.

8. POWIERZANIE I UDOSTĘPNIANIE DANYCH

1) Wdrożenie odpowiednich środków organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych obejmuje bezpieczeństwo związane z działaniami pracowników oraz zleceniobiorców.

2) W celu zapewnienia poufności Administrator ogranicza dostęp do danych osobowych dla osób, które nie przetwarzają danych w jego imieniu (podmioty przetwarzające) lub na jego polecenie (pracownicy, praktykanci, stażyści, wolontariusze). Zapewnienie bezpieczeństwa związane jest także z wysokim poziomem wiedzy osób upoważnionych.

8.1. PRZETWARZANIE DANYCH W IMIENIU ADMINISTRATORA

1) Outsourcing usług wiąże się z podpisaniem umowy działania w imieniu Administratora zgodnie z art. 28 RODO (tzw. umowa powierzenia danych). Sama umowa świadczenia usługi powinna określać usługi, które ma wykonywać usługodawca oraz ich parametry techniczne, ponieważ jest to prawnie wiążący kontrakt pomiędzy dostawcą i szkołą.

2) Administrator powierzając realizację swoich zadań podmiotom przetwarzającym (osobom lub podmiotom na podstawie umowy zlecenia - umowy cywilnoprawnej) ma obowiązek sprawdzić (np. przy pomocy ankiety lub audytu) czy podmiot przetwarzający daje gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych spełniających wymogi RODO i chroniących prawa osób, których dane dotyczą.

3) Administrator lub upoważniony przez niego audytor ma prawo przeprowadzania audytu w podmiotach przetwarzających w zakresie przetwarzania danych osobowych w imieniu Administratora.

4) Podmiot przetwarzający może rozpocząć realizacje swoich zadań po uprzednim uzyskaniu upoważnienia i polecenia na przetwarzanie danych osobowych Administratora zawartym w umowie lub innym instrumencie prawnym.

5) Podmiot przetwarzający może w ramach podpowierzania korzystać z usług innych podmiotów przetwarzających pod warunkiem uzyskania zgody Administratora.

6) Procedura przetwarzania danych w imieniu ADO stanowi **załącznik nr 8** do niniejszej Polityki.

7) Wzór umowy działania w imieniu Administratora (umowy powierzenia danych) pomaga skonstruować IOD i Radca prawny.

8) Informacja na temat każdej umowy powierzenia musi trafić do IOD, w celu aktualizacji RCP.

9) IOD prowadzi ewidencję podmiotów przetwarzających, której wzór stanowi **załącznik nr 8a** do niniejszego dokumentu.

8.2. UDOSTĘPNIANIE DANYCH

Dane osobowe są udostępniane innemu Administratorowi danych na wniosek o udostępnienie danych osobowych, zgodnie z procedurą udostępniania danych, która stanowi **załącznik nr 11** do niniejszej Polityki.

9. ORGANIZACJA SZKOLEŃ

1) Szkolenia dla Administratora oraz pracowników przeprowadza IOD, zgodnie z przygotowanym przez siebie planem szkoleń.

2) Nie rzadziej niż raz na trzy lata IOD przeprowadza szkolenie przypominające podstawowe zasady ochrony danych osobowych z ochrony danych osobowych dla wszystkich pracowników przetwarzających dane osobowe w szkole. Szkolenie, o którym mowa może być prowadzone w systemie samokształcenia.

3) Szkolenia dedykowane dla inspektora ochrony danych zapewniają Informacje Bezpieczne Sp. z o.o. zgodnie z podpisaną umową świadczenia usług.

4) Nowoprzyjęci pracownicy, których stałym miejscem wykonywania obowiązków służbowych jest szkoła, są szkoleni z zasad ochrony danych osobowych metodą samokształcenia. Przechodzą również szkolenie z obsługi systemu informatycznego, które przeprowadza ASI.

10. AUDYTY I INSPEKCJE

1) Inspekcje, audyty oraz monitorowanie przestrzegania RODO są jednym z głównych zadań Inspektora ochrony danych. Mają one za zadanie sprawdzenie prawidłowości przestrzegania przepisów określonych w niniejszym dokumencie. Monitorowaniu podlegają:

75) przestrzeganie zasad bezpieczeństwa określonych w POD;

76) korzystanie z systemów informatycznych;

77) wdrożone zabezpieczenia.

2) Celem przeprowadzanej kontroli jest doskonalenie środków technicznych i organizacyjnych mających wpływ na zabezpieczenie danych osobowych.

3) Nadzór nad ochroną danych osobowych sprawują:

78) IOD - w stosunku do wszystkich użytkowników;

79) ASI - w stosunku do użytkowników wykorzystujących do pracy systemy informatyczne;

4) Audyt ochrony danych może być planowy lub doraźny. Z audytu powstaje raport, pod którym podpisuje się audytujący i audytowany i który przedstawiany jest do zapoznania się Administratorowi danych.

11. NARUSZENIE OCHRONY DANYCH

1) Naruszenie bezpieczeństwa informacji to sytuacja zaistniała w wyniku niepożądanego lub nieoczekiwanego zdarzenia lub serii zdarzeń, skutkująca potencjalnie zwiększonym prawdopodobieństwem utraty lub faktyczną utratą przez informację (zarówno w postaci elektronicznej jak i papierowej) dowolnej z cech charakteryzujących jej bezpieczeństwo:

80) poufności – poprzez nieuprawniony dostęp do informacji lub jej ujawnienie;

81) integralności – poprzez nieuprawnioną modyfikację lub usunięcie informacji;

82) dostępności – poprzez brak dostępu w określonym czasie;

83) autentyczności – poprzez nieuprawnioną zmianę autora informacji.

2) Na możliwość wystąpienia naruszenia bezpieczeństwa informacji mogą wskazywać:

84) nietypowy stan pomieszczeń przetwarzania (naruszone plomby, otwarte pomieszczenia, okna, drzwi od szaf, biurek, włączone urządzenia, podłączane lub inaczej przyłączone przewody sieci logicznej);

85) zaginięcie sprzętu lub nośników informacji;

86) podejrzewane nieuzasadnione modyfikacje lub usunięcie danych;

87) nieprawidłowe lub nietypowe działanie systemu informatycznego, min.:

a) nietypowe komunikaty wyświetlane na monitorze;

b) odstająca od normy wydajność (prędkość) działania systemu;

c) brak możliwości zalogowania do systemu.

d) próby uzyskania informacji przez nieuprawnione osoby stosujące metody socjotechniczne.

3) Po stwierdzeniu wystąpienia lub podejrzeniu wystąpienia incydentu naruszenia bezpieczeństwa informacji pracownik powstrzymuje się od wszelkich czynności mogących zatrzeć ślady naruszenia bezpieczeństwa informacji, zwłaszcza od usuwania podejrzanego oprogramowania lub plików w systemie informatycznym, a w dalszej kolejności powiadamia:

88) bezpośredniego przełożonego;

89) Inspektora ochrony danych (iod.sp.puck@gmail.com).

4) ASI w przypadku naruszenia informacji w systemie informatycznym stosuje się do poleceń ww. powiadomionych osób, odpowiedzialnych za nadzór nad bezpieczeństwem informacji;

5) Pełna **procedura postępowania w przypadku naruszenia bezpieczeństwa informacji** znajduje się w **załączniku nr 4** do niniejszego dokumentu.

12. ZARZĄDZANIE RYZYKIEM INFORMACJI

6) Metodologa analizy ryzyka, proces analizy ryzyka oraz plan postępowania z ryzykiem opisany jest w osobnym dokumencie o nazwie: **Analiza ryzyka oraz ocena skutków planowanych operacji przetwarzania *w Szkole Podstawowej im. Mariusza Zaruskiego w Pucku***

13. OCENA SKUTKÓW

Metodologa oceny skutków oraz sam proces tej oceny przeprowadzony zostanie w osobnym dokumencie o nazwie: **Analiza ryzyka oraz ocena skutków planowanych operacji przetwarzania *w Szkole Podstawowej im. Mariusza Zaruskiego w Pucku***

14. ZAPEWNIENIE CIĄGŁOŚCI DZIAŁANIA

Dokument opisujący sposób w jaki szkoła zapewnia ciągłość działania w sytuacjach kryzysowych znajduje się w osobnym dokumencie przygotowanym wspólnie z informatykiem i przechowywanym u Dyrektora szkoły.

15. ZAŁĄCZNIKI

1) Zakres zadań i odpowiedzialności;

2) Instrukcja rozpatrywania żądań osób fizycznych

3) Wzory poleceń przetwarzania;

4) Procedura postępowania w sytuacji naruszenia ochrony danych osobowych

5) Wzór ewidencji osób

6) Procedura przyjęcia i zwolnienia pracownika (praktykanta, wolontariusza, stażysty).

7) Ochrona danych osobowych w fazie projektowania.

8) Procedura powierzenia danych podmiotom przetwarzającym i Ewidencja podmiotów przetwarzających.

9) Wzór druku zmiany haseł administracyjnych.

10) Procedura wykonania kopii zapasowych.

11) Procedura udostępniania danych osobowych.

12) Procedura współpracy z PUODO.

13) Procedura rekrutacji oraz wzory obowiązków informacyjnych i wzory zgód.

16. DOKUMENTY POWIĄZANE Z POLITYKĄ OCHRONY DANYCH

1) Rejestr czynności przetwarzania – Szkoły Podstawowej im. Mariusza Zaruskiego w Pucku

2) Analiza ryzyka oraz ocena skutków planowanych operacji przetwarzania w Szkole Podstawowej im. Mariusza Zaruskiego w Pucku

3) Plan ciągłości działania– Szkoły Podstawowej im. Mariusza Zaruskiego w Pucku

4) Plan szkoleń z ochrony danych osobowych– Szkoły Podstawowej im. Mariusza Zaruskiego w Pucku

5) Regulamin monitoringu – Szkoły Podstawowej im. Mariusza Zaruskiego w Pucku

6) Regulamin stosowania pracy zdalnej przez pracowników w Szkole Podstawowej im. Mariusza Zaruskiego w Pucku w związku z rozprzestrzenianiem się choroby zakaźnej wywołanej wirusem SARS-COV-2 zwanej „COVID-19"