

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

**Szkoły Podstawowej im. gen. Franciszka Kleeberga
w Kocku**

ul. Przechodnia 11, 21-150 Kock

*Niniejszy dokument jest wyłącznie dokumentem wewnętrznym stanowiącym własność administratora danych osobowych.

*Dokument zawiera zestaw praw, procedur i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych, wewnątrz jak i na zewnątrz Szkoły.

*Polityka odnosi się całościowo do problemu zabezpieczenia danych przetwarzanych tradycyjnie – w formie papierowej, jak i danych przetwarzanych w systemach informatycznych.

*Celem polityki jest wskazanie działań jakie należy wykonać oraz stanowi zasady i reguły postępowania, które należy stosować aby właściwie wykonywać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.

*Dokument stanowi tajemnicę Szkoły i nie należy go publikować, lecz rozpowszechniać jedynie wśród pracowników Szkoły.

SPIS TREŚCI

1. Definicje	4
2. Strategia i cele	5
3. Podstawa prawna.....	6
4. Deklaracja stosowania kierownictwa	6
5. Zasady przetwarzania danych.....	7
6. Procedura realizacji obowiązku informacyjnego	8
7. Procedura obsługi praw wynikających z RODO	8
8. Środki organizacyjne i techniczne	10
8.1. Środki organizacyjne	10
8.2. Środki techniczne	11
9. Strategie ochrony danych w fazie projektowania i fazy domyślnej	12
10. Szacowanie ryzyka dla danych osobowych i ocena skutków	14
10.1. Identyfikacja i klasyfikacja aktywów Szkoły	14
10.2. Zasady zarządzania aktywami	15
10.3. Szacowanie ryzyka.....	15
11. Organizacja przetwarzania danych osobowych (wewnątrz szkoły)	16
11.1. Zasady nadawania upoważnienia do przetwarzania danych.....	16
11.2. Zasady odbierania upoważnień do przetwarzania danych	17
12. Organizacja przetwarzania danych osobowych (na zewnątrz szkoły)	17
12.1. Udostępnianie danych.....	17
12.2. Przetwarzanie danych przez organ prowadzący szkołę	18
12.3. Powierzenie przetwarzania danych osobowych	18
13. Procedura rekrutacyjna	19
14. Procedura dostępu do pomieszczeń szczególnie chronionych	20
15. Procedura pracy na urządzeniach przenośnych	20
16. Procedura pracy na komputerach prywatnych	21
17. Procedura korzystania z sieci internet.....	22
18. Procedura tworzenia oraz zmiany hasła.....	22
18.1. Tworzenie hasła	22
18.2. Zmiana i przechowywanie hasła.....	23
19. Obsługa konta poczty elektronicznej	23
20. Aktualizacja oprogramowania	24
21. Kopie zapasowe	25
22. Archiwizacja	25
23. Konserwacja i naprawa sprzętu	26
24. Niszczenie dokumentów i utylizacja nośników	27



25. Utrzymanie czystości.....	27
26. Procedura postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych	28
26.1. Istota naruszenia ochrony danych osobowych	28
26.2. Postępowanie w przypadku naruszenia ochrony danych osobowych	29
26.3. Konsekwencje zaniechania zgłoszenia naruszenia ochrony danych.....	30
26.4. Udokumentowanie skutków oraz podjętych środków i działań	30
26.5. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu.....	31
26.6. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych	32
27. Postanowienia końcowe.....	32



1. DEFINICJE

1. **„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;
2. **„przetwarzanie”** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
3. **„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);
4. **„administrator - ADO”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
5. **„podmiot przetwarzający”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
6. **„inspektor – IOD”** oznacza osobę powołaną do pełnienia funkcji Inspektora Ochrony Danych w organizacji, inspektor odgrywa kluczową rolę w zakresie wspierania „kultury ochrony danych” oraz pomaga w implementacji niezbędnych elementów RODO w codziennej działalności organizacji. Administrator oraz podmiot przetwarzający zapewniają, by inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Inspektor bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Inspektor jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii oraz prawem państwa członkowskiego;
7. **„organ prowadzący szkołę”** oznacza ministra, jednostkę samorządu terytorialnego, inne osoby prawne i fizyczne,
8. **„pracownik”** oznacza każdą osobę świadczącą pracę na rzecz administratora na podstawie umowy o pracę oraz innych form zatrudnienia, upoważnioną do przetwarzania danych osobowych w organizacji,
9. **„polityka – PBDO”** oznacza dokument Polityki Bezpieczeństwa Danych Osobowych, jest to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych, wewnątrz określonej organizacji. Polityka odnosi się całościowo do problemu zabezpieczenia danych przetwarzanych tradycyjnie – w formie papierowej, jak i danych przetwarzanych



w systemie informatycznym. Celem polityki jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować aby właściwie wykonywać obowiązki administratora w zakresie zabezpieczenia danych osobowych;

10. „**zgoda**” oznacza 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;
11. „**naruszenie ochrony danych osobowych**” oznacza 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;

2. STRATEGIA I CELE

Szkoła realizuje cele i zadania określone w ustawie o systemie oświaty oraz w przepisach wykonawczych wydanych na jej podstawie, uwzględniające program wychowawczy i program profilaktyki dostosowany do potrzeb rozwojowych uczniów oraz potrzeb środowiska. Ponadto, Szkoła umożliwia realizację obowiązku szkolnego określonego w ustawie o systemie oświaty i jako szkoła publiczna:

1. zapewnia bezpłatne nauczanie w zakresie ramowych planów nauczania,
2. przyjmuje uczniów zamieszkałych w obwodzie szkoły oraz w uzasadnionych przypadkach uczniów z innych obwodów na zasadach określonych w statucie dotyczących rekrutacji uczniów, w ramach wolnych miejsc,
3. zatrudnia nauczycieli posiadających kwalifikacje określone w odrębnych przepisach,
4. realizuje określone w rozporządzeniu podstawy programowe,
5. zapewnia uczniom pomoc psychologiczną i pedagogiczną.

Nadrzędnym celem działań edukacyjnych szkoły jest wszechstronny rozwój ucznia. Szczegółowymi celami szkoły są:

1. zapewnienie uczniom pełnego rozwoju umysłowego, moralnoemocjonalnego i fizycznego w zgodzie z ich potrzebami i możliwościami psychofizycznymi, w warunkach poszanowania ich godności osobistej oraz wolności światopoglądowej i wyznaniowej,
2. przyswojenie przez uczniów określonego zasobu wiadomości na temat faktów, zasad, teorii i praktyki, niezbędnego do nauki na wyższych szczeblach edukacji,
3. zdobycie przez uczniów umiejętności wykorzystywania posiadanych wiadomości podczas wykonywania zadań i rozwiązywania problemów,
4. rozwijanie i przekształcanie spontanicznej motywacji poznawczej w motywację świadomą, przygotowanie ucznia do podejmowania zadań wymagających systematycznego i dużego wysiłku intelektualnego i fizycznego, wdrażanie go do przejmowania odpowiedzialności za własne zdrowie, rozwój i proces uczenia się,
5. rozbudzanie i rozwijanie wrażliwości estetycznej i moralnej dziecka oraz jego zdolności twórczych,
6. kształtowanie u uczniów postaw warunkujących sprawne i odpowiedzialne funkcjonowanie we współczesnym świecie,



7. kształtowanie systemu wartości opartego na: dobru, prawdzie, sprawiedliwości, uczciwości, poczuciu odpowiedzialności, szacunku do pracy, tolerancji, wrażliwości na innych oraz miłości do Ojczyzny i polskiego dziedzictwa kulturowego, przy jednoczesnym otwarciu na wartości kultur Europy i świata,
8. utrzymywanie bezpiecznych i higienicznych warunków pracy i nauki,
9. wspieranie rodziny w procesie wychowawczym,
10. stałe podnoszenie jakości pracy, motywowanie pracowników do ustawicznego rozwoju zawodowego i osobowego.

3. PODSTAWA PRAWNA

Akty prawne:

1. 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 Osobowych – RODO).
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych Dz.U. 2018 poz. 1000.
3. Ustawa z dnia 17 lutego 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne Dz. U. 2014 poz. 1114.
4. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U.2017.2247.

Inne dokumenty:

1. Norma PN-EN ISO 19011:2012.
2. Norma PN-EN ISO/IEC 27001:2017-06.
3. Norma PN-EN ISO/IEC 27002.
4. Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony M.P. 2018 poz. 827.
5. Wytyczne Grupy Roboczej Art. 29.
6. Bieżące wskazówki UODO oraz Ministerstwa Cyfryzacji.

4. DEKLARACJA STOSOWANIA KIEROWNICTWA

Zmieniająca się rzeczywistość prawna związana z obowiązywaniem RODO wymusiła na administratorze inwentaryzację zasobów danych osobowych i procesów ich przetwarzania. Z uwagi na pojawienie się nowych regulacji administrator deklaruje, że wdroży niezbędne procedury oparte na zasadach i podstawach przetwarzania zawartych w obowiązujących przepisach dotyczących ochrony danych osobowych.

Administrator świadomy wagi problemów i zagrożeń związanych z ochroną danych osobowych, w celu właściwej i skutecznej ochrony tych danych, wprowadza Politykę Bezpieczeństwa Danych Osobowych zwaną dalej „Polityką Bezpieczeństwa”. Opracowanie niniejszego dokumentu wynika ze zrozumienia znaczenia bezpieczeństwa danych we współczesnym świecie. Polityka Bezpieczeństwa zawiera wypracowane reguły i procedury takie jak:

- a. reguły bezpiecznego przechowywania danych osobowych,
- b. procedura udostępniania danych osobowych (wewnątrz oraz na zewnątrz),
- c. procedura realizacji uprawnień wynikających z RODO,
- d. stosowanie zasady privacy by design, privacy by default.

Ponadto, administrator zobowiązuje się do prowadzenia nadzoru nad przestrzeganiem założeń niniejszego dokumentu. W tym celu ustala coroczny plan sprawdzeń oraz wprowadza obowiązek cyklicznych szkoleń z zakresu ochrony danych osobowych oraz wprowadzonych w Szkole procedur bezpiecznego przetwarzania danych podnoszących świadomość pracownika.

W związku z pojawiającymi się zagrożeniami wynikającymi z rozwoju technologicznego administrator zobowiązuje się do cyklicznego szacowania ryzyka związanego z procesami przetwarzania danych osobowych.

5. ZASADY PRZETWARZANIA DANYCH

Każdy upoważniony do przetwarzania danych osobowych w imieniu administratora jest zobowiązany do przestrzegania poniższych reguł:

1. Pracownik jest zobowiązany do przetwarzania danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.
2. Pracownik przed zebraniem danych osobowych od osoby fizycznej zobowiązany jest do umożliwienia zapoznania się z klauzulą informacyjną zawierającą wszelkie informacje dotyczące operacji przetwarzania oraz jej celach.
3. Pracownik czuwa by dane osobowe były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
4. Jeżeli pozyskane dane osobowe mają być wykorzystane w innym celu niż cel, w którym zostały zebrane, przed takim dalszym przetwarzaniem pracownik zobowiązany jest do poinformowania o tym zamiarze osoby, których dane dotyczą oraz udzielenia im wszelkich innych stosownych informacji tj. o przysługujących prawach, nowym celu przetwarzania, podstawie przetwarzania.
5. Dane osobowe gromadzone przez pracownika w Szkole muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do realizacji celów, w których są przetwarzane.
6. Pracownik odpowiada za zakres przetwarzanych danych. Zakazuje się gromadzenia danych zbędnych dla osiągnięcia określonego celu przetwarzania danych tj. nadmiarowych.
7. Pracownik nadzoruje by dane osobowe były prawidłowe i w razie konieczności je uaktualnia.
8. Pracownik winien podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.



9. Administrator odpowiada za wprowadzenie procedur wyznaczających terminy przechowania danych (okresy retencji) lub procedur określających terminy okresowych przeglądów danych, a pracownik zobowiązany jest do ich przestrzegania.
10. Pracownik ma obowiązek przetwarzać dane w sposób zapewniający odpowiednie bezpieczeństwo w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

6. PROCEDURA REALIZACJI OBOWIĄZKU INFORMACYJNEGO

W celu wypełnienia obowiązku informacyjnego wprowadza się następujące reguły:

1. Przed podjęciem działań z danymi osobowymi należy umożliwić osobie, zapoznanie się z klauzulą informacyjną.
2. Informowanie powinno się dokonać bez prośby zainteresowanego.
3. Obowiązek informacyjny spełnia się poprzez pozostawienie treści klauzuli w miejscu dostępnym dla osób fizycznych, od których pozyskiwane są dane osobowe tj. sekretariacie Szkoły oraz poprzez zamieszczenie treści klauzuli informacyjnej na stronie internetowej, w Biuletynie Informacji Publicznej.
4. Treść klauzuli należy skonsultować każdorazowo z inspektorem w celu potwierdzenia zgodności z obowiązującymi przepisami prawa.
5. Treść klauzuli informacyjnej jest zamieszczana w regulaminach konkursów i innych wydarzeń kulturalnych.

7. PROCEDURA OBSŁUGI PRAW WYNIKAJĄCYCH Z RODO

Obsługa uprawnień, które zostały zawarte w przepisach rozdziału III RODO stanowi gwarancję poszanowania praw i wolności osób fizycznych i jako podstawowe prawo realizowane jest poprzez wypełnienie poniższych reguł.

1. Administrator gwarantuje by wszelkie przekazywane informacje były sformułowane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
2. Administrator w miejscu ogólnodostępnym (w tym na stronie internetowej) zamieszcza informację, do kogo i w jakiej formie należy kierować żądanie realizacji praw.
3. Realizacja żądania osób fizycznych w zakresie realizacji praw wynikających z RODO (a w szczególności wskazanych w klauzuli informacyjnej) należy do obowiązków inspektora.
4. Zgłoszenie żądania osoby fizycznej powinno zawierać:
 - a. imię, nazwisko osoby której zgłoszenie dotyczy,
 - b. opis zgłaszanego żądania wraz ze wskazaniem ewentualnych zastrzeżeń,
 - c. podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
 - d. pełnomocnictwo jeśli w imieniu zgłaszającego żądanie kieruje pełnomocnik,
 - e. informacje o preferowanej formie odpowiedzi, jeżeli kanał odpowiedzi ma być inny niż zgłoszone żądanie.

5. Pracownik może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby składającej żądanie w przypadku, gdy ma co do niej uzasadnione wątpliwości.
6. Przed realizacją zgłoszenia, pracownik zobowiązany jest zweryfikować czy osoba występująca z żądaniem realizacji jej praw, jest osobą której dane dotyczą. Weryfikacja może polegać na:
 7. Potwierdzeniu w rozmowie telefonicznej danych posiadanych przez Szkołę,
 8. Wgląd w dokument zawierający dane osobowe, potwierdzające tożsamość osoby.
9. Jeżeli zgłoszenie nastąpiło w formie ustnej, pracownik zobowiązany jest do sporządzenia notatki, zawierającej dane o których mowa w punkcie 4.
10. Po otrzymaniu zgłoszenia, pracownik zobowiązany jest poinformować osobę występującą z wnioskiem o realizację jego praw o przyjętym zgłoszeniu.
11. W przypadku skierowania żądania realizacji praw bezpośrednio pracownikowi, zobowiązany jest on najpóźniej w terminie 7 dni przesłać treść żądania inspektorowi.
12. Pracownik jest zobowiązany do udzielania informacji inspektorowi niezbędnych do realizacji żądania osoby fizycznej.
13. Wprowadza się obowiązek rejestracji każdego wniosku o realizację praw osób wpływający bezpośrednio do siedziby Szkoły lub na skrzynki mailowe pracowników, poprzez wpisanie do rejestru obsługi praw osób fizycznych wraz ze wskazaniem daty otrzymania wniosku.
14. W przypadku, gdy żądanie osoby fizycznej nie może zostać uwzględnione pracownik informuje ją w ww. terminach o odmowie realizacji żądania wraz z podaniem przyczyn oraz o możliwości wniesienia skargi do organu nadzorczego.
15. Wszelkie informacje oraz komunikacja i działania podejmowane w związku z realizacją praw osób są bezpłatne.
16. Pracownik może zażądać od osoby fizycznej uiszczenia opłaty w wysokości uwzględniającej koszty udzielenia odpowiedzi w przypadku, gdy żądania są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na nagminny charakter - ale wyłącznie po uzyskaniu uprzedniej zgody administratora na takie działanie i konsultacji z IOD.
17. Odpowiedź na żądanie osoby fizycznej realizowana jest na piśmie lub drogą elektroniczną bądź w sposób wskazany przez osobę, której prawa dotyczą.
18. W przypadku przekazywania informacji drogą elektroniczną pracownik przesyła dane w sposób zapewniający ich bezpieczeństwo tj. po uprzednim nadaniu hasła odczytu do przesyłanego pliku.
19. Pracownik nie powinien wydawać skanów dokumentów albo ich kserokopii, gdyż mogą zawierać dodatkowe dane nie dotyczące osoby występującej z wnioskiem.
20. W razie konieczności wydania kserokopii dokumentów, wydanie następuje po uprzednim zanonimizowaniu danych innych osób zawartych w dokumencie oraz konsultacji z IOD.
21. Pracownik zanim zrealizuje żądanie osoby fizycznej zobowiązany jest każdorazowo do weryfikacji zasadności zgłaszanego żądania, jego zakresu oraz podstawy realizacji obowiązku z przepisami RODO. Analiza w szczególności obejmuje wyłączenia realizacji praw z uwagi na interes administratora.
22. Jeżeli żądanie osoby fizycznej wpłynie na skrzynkę iod@pcat.pl wówczas IOD przesyła wniosek pracownikowi odpowiedzialnemu za udzielenie informacji. Pracownik otrzymujący zgłoszenie postępuje według opisanej powyżej procedury.



8. ŚRODKI ORGANIZACYJNE I TECHNICZNE

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża niniejsze środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem RODO i aby móc to wykazać.

8.1. ŚRODKI ORGANIZACYJNE

1. Opracowano i wdrożono Politykę Bezpieczeństwa.
2. Opracowano i wdrożono procedurę postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.
3. Powołano Inspektora Ochrony Danych.
4. Zastosowano upoważnienia adekwatne do zakresu przetwarzania zgodnego z zajmowanym stanowiskiem służbowym.
5. Upoważnienia do przetwarzania danych pracowników mających dostęp do pomieszczeń szczególnie chronionych, zawierają szczegółowe umocowania.
6. Wprowadzono ewidencję upoważnień pracowników.
7. W ewidencji upoważnień prowadzi się rejestr osób, które upoważniono do dostępu do pomieszczeń szczególnie chronionych.
8. Wprowadzono obowiązek odbierania oświadczenia pracowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi regulacjami bezpieczeństwa danych osobowych administratora wraz z obowiązkiem zachowania poufności wszelkich informacji uzyskanych w ramach wykonywanych obowiązków, również po ustaniu zatrudnienia.
9. Wprowadzono obowiązek bezpiecznego udostępniania danych osobowych podmiotom zewnętrznym poprzez zawieranie umów powierzenia (lub innych instrumentów prawnych) oraz zobowiązania do zachowania danych osobowych w poufności.
10. Wprowadzono obowiązek cyklicznego szkolenia pracowników z obowiązujących przepisów dotyczących ochrony danych osobowych jak i wewnętrznych regulacji bezpieczeństwa danych osobowych stosowanych przez administratora.
11. Wprowadzono obowiązek cyklicznego szkolenia pracowników w zakresie bezpiecznej obsługi urządzeń i programów służących do przetwarzania danych osobowych.

Zabezpieczenia we własnym zakresie

Pracownik zobowiązany jest do przestrzegania zasady czystego biurka i ekranu w szczególności poprzez:

1. Schowanie wszystkich dokumentów, nośników zawierających dane osobowe w miejsce niedostępne dla innych osób w trakcie pracy, w trakcie sprzątania pomieszczeń oraz po zakończeniu pracy.
2. Dbanie o porządek, poprzez pozostawienie na stanowisku pracy wyłącznie dokumentów, które są niezbędne do wykonywania czynności służbowych.
3. Blokowanie dostępu lub wylogowanie się z systemu przy czasowym opuszczaniu stanowiska pracy.



4. Zamknięcie wszystkich aplikacji, wylogowanie się z systemu i wyłączenie komputera po zakończeniu pracy.
5. Zachowanie porządku na pulpicie komputera poprzez cotygodniowy przegląd połączony z porządkowaniem oraz usuwaniem zbędnych folderów i plików znajdujących się na pulpicie systemu.

Pracownik zobowiązany jest również do:

1. Nieprzechowywania plików prywatnych (w tym poczty prywatnej, zdjęć, dokumentów prywatnych, skanów etc.) na powierzonym sprzęcie elektronicznym tj. komputerach, telefonach, aparatach fotograficznych.
2. Wylogowania się z systemu operacyjnego lub używanego programu przy każdorazowym odejściu od komputera.
3. Pilnego strzeżenia dokumentów w formie papierowej, płyt CD/DVD, pamięci i komputerów przenośnych, oraz wszelkich innych urządzeń przenośnych, na których mogą znajdować się dane osobowe.
4. Nieużywania powtórnie dokumentów zadrukowanych jednostronnie.
5. Niezapisywania hasła wymaganego do uwierzytelnienia się w systemie informatycznym na papierze lub innym nośniku.
6. Nieudostępniania hasła wymaganego do uwierzytelnienia się do systemu informatycznego innym osobom, w tym zarówno pracownikom Szkoły jak i osobom postronnym.
7. Dbania o prawidłową wentylację komputerów (zabrania się zasłaniania kratki wentylatorów meblami, zasłonami lub stawiania komputerów tuż przy ścianie).
8. Niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory).
9. Powstrzymywania się od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych.
10. Przestrzegania przez pracowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń osoby nadzorującej system informatyczny.
11. Niszczona w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy.
12. Zamykania szafek z dokumentami i drzwi na klucz po zakończeniu pracy w danym dniu.

8.2. ŚRODKI TECHNICZNE

1. Dane osobowe przechowywane są w uporządkowanych zbiorach tj. księgozbiorach, katalogach, skoroszytach, segregatorach, itp.
2. Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zamykanymi na klucz.
3. Pomieszczenia, w których przetwarza się dane są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.

Dokumenty papierowe

1. Dane w formie papierowej przechowywane są w zamkniętych metalowych szafach.

2. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów, uniemożliwiających ich odtworzenie.

Dokumenty elektroniczne

1. Dokumenty elektroniczne przechowywane są na zabezpieczonych urządzeniach końcowych.
2. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
3. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity, w postaci programów antywirusowych.
4. Użyto systemu Firewall do ochrony dostępu do sieci komputerowej.
5. W sytuacji braku możliwości stosowania mechanizmu wymuszającego zmianę haseł dostępu do systemu informatycznego, w którym przetwarzane są dane osobowe administrator wprowadza procedurę ustanawiania i zmiany hasła.
6. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
7. ADO zobowiązany jest wyznaczyć pracownika odpowiedzialnego za mechanizm tworzenia kopii zapasowych z systemu informatycznego i wprowadzić obowiązek tworzenia kopii zapasowych.

9. STRATEGIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA I FAZIE DOMYŚLNEJ

Uwzględniając koncepcje ochrony danych w fazie projektowania administrator już podczas planowania systemu ochrony danych osobowych wdraża takie środki, by od samego początku chronić przetwarzane dane oraz prywatność osób, których dane dotyczą. W tym celu administrator wprowadza następujące reguły:

1. Każde planowane przedsięwzięcie w Szkole musi zostać poprzedzone analizą wpływu planowanych zmian na bezpieczeństwo danych osobowych.
2. Jako planowane procesy, w których administrator zobowiązany jest wziąć pod uwagę bezpieczeństwo danych osobowych wyróżnia się w szczególności:
 - a. przystąpienie do przetargu w ramach zamówień publicznych,
 - b. przystąpienie do projektów realizowanych ze środków europejskich,
 - c. przeprowadzenie nowych akcji marketingowych,
 - d. zakup nowego systemu bądź aktualizacja obecnego systemu informatycznego,
 - e. zakup nowych systemów ochrony fizycznej (systemy alarmowe, monitoring) jak i systemów bezpieczeństwa IT,
 - f. wprowadzenie nowych technologii produkcyjnych i organizacyjnych,
 - g. zatrudnienie nowych pracowników,
 - h. zmiana celów przetwarzania.
3. Administrator bądź wyznaczony przez niego pracownik zobowiązany jest na etapie planowania procesu wdrożyć odpowiednie środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych, a w szczególności zobowiązany jest do stosowania:
 - a. pseudonimizacji,
 - b. szyfrowania,



- c. minimalizacji danych,
 - d. prawidłowości i przejrzystości zbieranych danych,
 - e. ograniczenia do niezbędnej ilości zbieranych danych osobowych,
 - f. ograniczenia do niezbędnego zakresu przetwarzania danych,
 - g. ograniczenia do niezbędnego okresu przechowywania danych,
 - h. technik zapewniających odpowiedni poziom dostępności,
4. Na etapie planowania procesów administrator bądź wyznaczony przez niego pracownik zobowiązany jest również:
- a. rozważyć na jakiej przesłance legalności zostanie oparty proces przetwarzania danych, przy czym jeśli będzie to zgoda należy przygotować odpowiednio wcześniej jej treść oraz ustalić sposób jej zbierania i odwołania,
 - b. opracować treść oraz sposób przekazania klauzul zawierających obowiązek informacyjny,
 - c. administrator zobowiązany jest poinformować inspektora o wszystkich planowanych przedsięwzięciach oraz umożliwić mu podjęcie wszelkich koniecznych działań niezbędnych do zapewnienia bezpieczeństwa przetwarzania danych osobowych,
 - d. przy wyborze kontrahenta, partnera biznesowego, kooperanta administrator powinien rozważyć, który z nich w najpełniejszy sposób realizuje zasadę bezpiecznego przetwarzania danych osobowych,
 - e. przy wyborze nowego systemu informatycznego, systemu ochrony bądź wprowadzaniu zmian technologicznych administrator powinien kierować się również zapewnieniami producenta dotyczącymi bezpieczeństwa przetwarzania danych osobowych oraz dostosowaniu do wymogów RODO.

Administrator świadomy jest, że zasada ochrony danych w fazie projektowania nie ogranicza się jedynie do procesu planowania, gdyż z przepisów RODO jasno wynika, że ocena zgodności z przepisami dotyczy również etapu realizacji procesu. Wobec powyższego administrator wprowadza zasadę regularnego przeglądu funkcjonowania procesów przetwarzania danych oraz jego elementów składowych poprzez:

1. Sprawdzenie poprawności metod zbierania i przechowywania zgód na przetwarzanie danych osobowych (w tym zasadność ich zbierania, możliwość ich wycofania oraz treści samej zgody).
2. Sprawdzenie realizacji wypełniania obowiązków informacyjnych.
3. Audyty procesów przetwarzania danych osobowych pod względem adekwatności ich przetwarzania oraz ograniczenia do niezbędnej ilości zbieranych danych. W tym celu administrator zobowiązuje:
 - a. pracowników odpowiedzialnych za umieszczenie informacji publicznych na stronie Biuletynu Informacji Publicznej (BIP) zobowiązuje do przeglądu umieszczanych na stronie treści pod kątem prawidłowej anonimizacji umieszczanych danych w następujący sposób
 - b. pracowników odpowiedzialnych za prowadzenie rekrutacji zobowiązuje do przestrzegania procedury rekrutacyjnej określonej w niniejszej Polityce Bezpieczeństwa,
 - c. pracowników odpowiedzialnych za prowadzenie projektów realizowanych z funduszy unijnych zobowiązuje do czuwania nad realizacją obowiązków, które spoczywają na Szkole jako administratorze danych przetwarzanych w projekcie (np. w zakresie spełnienia obowiązku informacyjnego),



- d. pracowników do wykonywania cyklicznej inwentaryzacji zasobów poczty służbowej i usuwania wiadomości, które utraciły znaczenia dla wypełniania obowiązków służbowych.

Realizując zasadę ochrony prywatności i bezpieczeństwa jako właściwości domyślnych (*privacy by default*) administrator bądź pracownik nadzorujący pracę systemu informatycznego zobowiązany jest do:

1. Konfiguracji systemu informatycznego w taki sposób, aby od momentu jego uruchomienia system zapewniał odpowiedni poziom ochrony według ustawień domyślnych.
2. Konfiguracja systemu informatycznego powinna zapewniać:
 - a. aby system nie pozwalał na zbieranie nadmiernej ilości danych osobowych,
 - b. aby system wskazywał bądź umożliwiał wprowadzenie danych dotyczących okresu przechowywania danych,
 - c. aby system umożliwiał dostęp do danych jedynie upoważnionym w danym zakresie pracownikom.
3. Wprowadzenia zakazu dokonywania jakichkolwiek samodzielnych zmian przez pracowników w ustawieniach fabrycznych komputerów oraz w ustawieniach systemu informatycznego.

10. SZACOWANIE RYZYKA DLA DANYCH OSOBOWYCH I OCENA SKUTKÓW

Administrator powinien przeprowadzić ogólną ocenę ryzyka oraz szczegółową ocenę ryzyka, ukierunkowaną na skutki w zakresie naruszenia praw lub wolności osób fizycznych (tzw. ocenę skutków dla ochrony danych).

Ogólną ocenę ryzyka w zakresie bezpieczeństwa przetwarzania informacji, w tym danych osobowych, należy przeprowadzić, biorąc pod uwagę potencjalne negatywne skutki (straty materialne i niematerialne) zarówno dla Administratora, jak i osób, których dane dotyczą. Ocenę skutków dla ochrony danych przeprowadza się natomiast wtedy, gdy istnieje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą.

10.1. IDENTYFIKACJA I KLASYFIKACJA AKTYWÓW SZKOŁY

Zarządzanie aktywami, jest realizowane w celu zapewnienia wymaganego poziomu bezpieczeństwa ochrony danych osobowych. Należy zidentyfikować i sklasyfikować wszystkie aktywa Szkoły, które wiążą się z przetwarzaniem danych osobowych. Aktywa to wszystko, co ma wartość dla Szkoły, rozumieć przez to należy zarówno informacje, w tym dane osobowe, jak i inne zasoby Szkoły, takie jak: posiadana wiedza, personel, sprzęt, oprogramowanie oraz inne środki techniczne i organizacyjne związane z przetwarzaniem danych osobowych. Identyfikacja i klasyfikacja aktywów w danej organizacji powinna być przeprowadzana na takim poziomie szczegółowości, aby zapewnić niezbędne informacje wymagane w procesie szacowania ryzyka. Posługując się schematem zaczerpniętym z normy ISO/IEC 27005, aktywa te można podzielić na podstawowe i wspierające. Aktywa podstawowe to procesy i działania biznesowe oraz informacje. Aktywa wspierające to sprzęt, oprogramowanie, sieć, personel, siedziba, struktura organizacyjna. Aktywa są chronione ze względu na wymagania wynikające zarówno z przepisów prawa oraz regulacji wewnętrznych, z których wynika ochrona właściwych aktywów, a także z zasad bezpieczeństwa wymaganych przez Szkołę, postanowień umów pomiędzy Szkołą, a podmiotami zewnętrznym czy z warunków licencji.



10.2. ZASADY ZARZĄDZANIA AKTYWAMI

Zarządzanie aktywami w Szkole odbywa się zgodnie z poniższymi zasadami:

1. Ustalenie odpowiedzialności za aktywa: należy określić właścicieli wszystkich aktywów oraz przydzieloną im odpowiedzialność za utrzymanie odpowiednich zabezpieczeń. Wdrożenie określonych zabezpieczeń może być delegowane przez właściciela aktywów, jednak pozostaje on nadal odpowiedzialny za adekwatną ochronę aktywów.
2. Identyfikacji aktywów: w wyniku identyfikacji aktywów powinno się uzyskać listę aktywów istotnych z punktu widzenia zarządzania ryzykiem oraz listę procesów biznesowych, w których aktywa te są wykorzystywane. Kolejnym istotnym krokiem podczas identyfikacji aktywów jest określenie ich wartości.
3. Akceptowalnego użycia aktywów: w dokumentacji są określone i wdrażane przez administratora zasady dopuszczalnego korzystania z aktywów i zasobów związanych z przetwarzaniem danych osobowych,
4. Klasyfikacji aktywów (szczegółowy opis stosowanych zabezpieczeń): określona jest metoda oraz sposób klasyfikacji aktywów odzwierciedlający wymagania ich ochrony na odpowiednim poziomie.
5. Oznaczania aktywów: stosowane są regulacje wewnętrzne wyznaczające zasady oznaczanie aktywów informacji i postępowania z nimi.

10.3. SZACOWANIE RYZYKA

1. Szacowanie ryzyka ma na celu określenie, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i jak dotkliwe straty mogą powstać. W ramach tego działania dla zidentyfikowanych procesów przetwarzania danych i występujących tam aktywów należy wskazać, przeanalizować i oszacować:
 - a. występujące zagrożenia dla bezpieczeństwa przetwarzanych danych,
 - b. zastosowane środki bezpieczeństwa,
 - c. podatność przyjętych rozwiązań z uwzględnieniem zastosowanych środków bezpieczeństwa na urzeczywistnienie się zidentyfikowanych zagrożeń,
 - d. potencjalne następstwa w przypadku zaistnienia określonych zagrożeń.
2. Proces zarządzania ryzykiem w bezpieczeństwie informacji realizuje się zgodnie z wytycznymi normy PN-ISO/IEC 27005:2014.
3. Wszyscy pracownicy podczas realizacji zadań biorą pod uwagę ryzyka związane z bezpieczeństwem przetwarzania danych.
4. Administrator zobowiązany jest do:
 - a. identyfikacji i klasyfikacji aktywów oraz zasobów informacyjnych na potrzeby analizy szacowania ryzyka,
 - b. identyfikacji scenariuszy wykorzystania podatności na zagrożenie,
 - c. szacowania strat dla zasobów użytych w realizacji procesów objętych przeglądem analizy ryzyka,
 - d. wykonania oceny skutków zgodnie z art. 35 RODO dla operacji przetwarzania danych osobowych (jeżeli jest wymagana przepisami prawa)
 - e. wykonania analizy szacowania ryzyka i przeprowadzenia oceny skutków zgodnie z art. 35 RODO, w przypadku wdrożenia nowej technologii (np. nowego systemu informatycznego) w Szkole służącej do przetwarzania danych osobowych,



- f. w razie potrzeby po dokonaniu oceny skutków, przeprowadzenia zgodnie z art. 36 RODO konsultacji z Urzędem Ochrony Danych Osobowych w sytuacji, gdy Administrator nie jest w stanie zminimalizować wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.
5. Zadania inspektora oraz pracownika nadzorującego system informatyczny:
 - a. przygotowanie Procedury szacowania ryzyka
 - b. przygotowanie wykazu aktywów Szkoły wraz z ich klasyfikacją,
 - c. przeprowadzenie analizy szacowania ryzyka i przygotowanie raportu (wyników) szacowania ryzyka w Rejestrze ryzyka,
 - d. przygotowanie planu postępowania z ryzykami,
 - e. ewentualne konsultowanie oceny skutków i wsparcie administratora w jej wykonaniu.
6. Zadania Administratora:
 - a. zatwierdzenie wykazu aktywów Szkoły (informacyjnych),
 - b. zatwierdzenie rejestru ryzyka Szkoły,
 - c. zatwierdzenie planów postępowania z ryzykami,
 - d. przeprowadzenie i zatwierdzenie oceny skutków (jeżeli została wykonana).

Ocena skutków jest wykonywana zgodnie z metodologią wskazaną przez Urząd Ochrony Danych Osobowych.

11. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH (WEWNĄTRZ SZKOŁY)

Szkoła realizując niniejszą Politykę Bezpieczeństwa w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie pracownikom (w niektórych przypadkach praktykantom, stażystom). Zezwolenie na przetwarzanie danych osobowych realizowane jest poprzez nadanie stosownego upoważnienia.

11.1. ZASADY NADAWANIA UPOWAŻNIENIA DO PRZETWARZANIA DANYCH

1. Upoważnienie do przetwarzania danych osobowych wydawane jest każdemu z pracowników osobno, w zakresie adekwatnym do pełnionych obowiązków służbowych.
2. Upoważnienia wydawane są na czas określony i ustają po terminie na jaki zostały wydane.
3. Od pracownika odbiera się oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi regulacjami bezpieczeństwa danych osobowych administratora.
4. Pracownika zobowiązuje się do zachowania w poufności wszelkich informacji uzyskanych w ramach wykonywanych obowiązków, również po ustaniu zatrudnienia.
5. Fakt nadawania upoważnienia jest odnotowywany w rejestrze upoważnień.
6. Administrator informuje o nadaniu upoważnienia do przetwarzania danych pracownikowi osobę nadzorującą system informatyczny, która nadaje dostęp do systemu informatycznego poprzez przydzielenie loginu i hasła.
7. Przydzielony login odnotowuje się w rejestrze upoważnień.

8. Nadane przez administrator upoważnienia mogą być modyfikowane w trakcie ich obowiązywania. Modyfikacja może nastąpić w skutek zmiany zakresu wykonywanych prac przez osobę upoważnioną.
9. Ewidencja osób upoważnionych do przetwarzania danych podlega przeglądowi każdorazowo z przeglądem organizacyjnych i technicznych środków bezpieczeństwa, czyli nie rzadziej niż raz w roku.

11.2. ZASADY ODBIERANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH

Upoważnienie do przetwarzania danych w określonych sytuacjach może być odebrane pracownikowi przez administratora:

1. Gdy pracownik posługuje się danymi w sposób niewłaściwy, przetwarza je w zakresie wykraczającym poza nadane upoważnienie.
2. Rażącego naruszenia zasad Polityki Bezpieczeństwa.
3. Rozwiązania stosunku pracy bądź innego stosunku prawnego łączącego osobę upoważnioną z administratorem.
4. Zmiany stanowiska pracy, na stanowisko uzasadniające konieczność posiadania upoważnienia w innym zakresie.

W sytuacji odebrania upoważnienia do przetwarzania danych stosuje się niniejsze zasady:

1. Administrator lub osoba wyznaczona informuje pracownika o przebiegu przekazywania obowiązków i rozliczeniu się tej osoby z pobranego sprzętu, materiałów i dokumentów należących do pracodawcy według przyjętych procedur.
2. Osoba nadzorująca system informatyczny blokuje dostęp pracownika do poczty elektronicznej oraz systemu informatycznego np.. poprzez zmianę hasła dostępu do poczty.
3. Pracownikowi odbiera się możliwość dostępu do budynków i pomieszczeń należących do szkoły.
4. W przypadku zmiany stanowiska pracy powyższe reguły stosuje się odpowiednio.
5. Fakt odebrania upoważnienia odnotowuje się w rejestrze upoważnień wraz ze wskazaniem daty.

12. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH (NA ZEWNĄTRZ SZKOŁY)

Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą administratora, dane osobowe mogą być udostępniane w następujących przypadkach:

- a. na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów,
- b. na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych,
- c. na podstawie wniosku osoby, której dane dotyczą.

12.1. UDOSTĘPNIANIE DANYCH

1. W przypadku udostępniania danych osobowych na zewnątrz administrator dokonuje oceny sposobu przygotowania danych, a także analizuje sposób i prawidłowość przygotowania danych do udostępnienia.

2. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.
3. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru np. e-mailem, listem poleconym za potwierdzeniem nadania lub innym bezpiecznym sposobem, pozwalającym na udokumentowanie spełnienia prawa.
4. Udostępniając dane osobowe innym podmiotom należy odnotowywać informacje o udostępnieniu bezpośrednio w systemie informatycznym, z którego udostępniono dane lub w inny zatwierdzony sposób.
5. Administrator prowadzi ewidencję podmiotów, którym udostępniono przetwarzane dane. Odnotować należy: informacje o odbiorcy danych, dacie i zakresie udostępnionych danych osobowych.

12.2. PRZETWARZANIE DANYCH PRZEZ ORGAN PROWADZĄCY SZKOŁĘ

Zgodnie z przepisami ustawy o systemie oświaty oraz ustawy Prawo oświatowe organ prowadzący szkołę ma dostęp (a szkoła mu ten dostęp zapewnia) do danych osobowych przetwarzanych w szkole w związku z realizacją swoich obowiązków wynikających z przepisów prawa.

1. Na potrzeby kontroli organ prowadzący szkołę ma prawo dostępu do objętej zakresem kontroli dokumentacji będącej w posiadaniu szkoły.
2. Organ prowadzący jest odrębnym od Szkoły administratorem danych osobowych przetwarzanych w związku z kontrolą Szkoły.
3. Osoba kontrolująca powinna mieć upoważnienie do przetwarzania danych osobowych w zakresie przeprowadzenia kontroli, nadane przez organ prowadzący.
4. Przed udostępnieniem danych organowi prowadzącemu Szkoła musi przeprowadzić analizę zakresu żądanych danych w stosunku do celu kontroli.
5. Jeżeli organ prowadzący szkołę zapewnia jej obsługę administracyjną, prawną, czy finansową, to szkoła, jako administrator danych, udostępnia dane w ramach powierzenia przetwarzania danych tylko w zakresie niezbędnym do realizacji tego celu oraz po spełnieniu wymogów określonych w art. 28 RODO.
6. Szkoła może przekazywać gromadzone przez siebie dane osobowe w postaci papierowej lub elektronicznej organowi prowadzącemu, jeżeli takie działanie ma odpowiednią podstawę prawną oraz spełnione zostały wymogi bezpieczeństwa danych osobowych
7. Organ prowadzący jest obowiązany przetwarzać pozyskane od szkoły dane w sposób zapewniający ich bezpieczeństwo.
8. Organ prowadzący szkołę nie może mieć dostępu do danych zawartych w aktach osobowych: nauczycieli, innych niż nauczyciele pracowników pedagogicznych.

12.3. POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej (w tym elektronicznej) umowy lub innego instrumentu prawnego, określającej w szczególności przedmiot i czas trwania przetwarzania oraz charakter i cel przetwarzania danych. Umowa musi określać również obowiązki

i zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub



nienależytego wykonania umowy. Regulacje dotyczące sposobu przetwarzania danych oraz obowiązków ciążących na stronach umowy winny zawierać również regulujące dotyczące:

1. Zobowiązania o zachowaniu poufności przez podmiot przetwarzający oraz osoby biorące udział w przetwarzaniu.
2. Obsługi praw jednostki, w szczególności obowiązków informowania administratora o otrzymaniu zgłoszenia i sposobie jego realizacji.
3. Niezwłocznego zgłaszania administratorowi wszelkich podejrzeń o naruszeniu ochrony powierzonych danych.
4. Sposób przekazania danych po zakończeniu trwania przetwarzania.
5. Realizacji uprawnień kontrolnych.
6. Dalszego powierzania danych przez podmiot przetwarzający.

Procedura zawarcia umowy powierzenia przetwarzania danych osobowych

1. Pracownik informuje administratora lub inspektora o potrzebie powierzenia danych osobowych do przetwarzania.
2. Inspektor w porozumieniu z pracownikiem przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.
3. Pracownik w projekcie umowy określa procesy przetwarzania powierzonych danych osobowych oraz ich zakres.
4. Sporządzony projekt umowy przedkłada administratorowi do podpisu.
5. Zawarta umowa powierzenia odnotowywana jest w rejestrze umów powierzenia.

13. PROCEDURA REKRUTACYJNA

Przetwarzanie danych osobowych kandydatów do pracy odbywa się z należyтым poszanowaniem prawa do prywatności wobec czego wprowadza się następujące zasady przy prowadzeniu rekrutacji:

1. Administrator (lub pracownik odpowiedzialny za rekrutację) zamieszczając ogłoszenie rekrutacyjne zobowiązany jest do zawarcia w jego treści klauzuli informacyjnej dotyczącej przetwarzania danych osobowych kandydata oraz oświadczeń tj.:
 - a. oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych zawartych w CV, liście motywacyjnym lub innych załączonych dokumentach (jeśli przekazane dane obejmują szczególne kategorie danych),
 - b. oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych w celu wykorzystania ich w kolejnych rekrutacjach prowadzonych przez Szkołę.
2. W przypadku braku zawarcia stosownej zgody w dokumentach aplikacyjnych pracownik kontaktuje się z kandydatem w celu odebrania stosownego oświadczenia o wyrażeniu zgody. Jeżeli pracownik nie uzyska oświadczenia, zobowiązany jest do usunięcia dokumentów aplikacyjnych w sposób trwały.
3. W przypadku wymagań wynikających z zapisów odpowiednich przepisów prawa, po zakończeniu procesu rekrutacji dokumenty zawierające dane osobowe kandydatów do pracy są archiwizowane zgodnie z zapisami tych przepisów.



4. Pracownik odpowiedzialny za rekrutację przechowuje dokumenty aplikacyjne w miejscu zabezpieczonym przed dostępem osób nieuprawnionych.
5. Administrator określił czas w jakim dokumenty aplikacyjne są przechowywane, tj. 9 miesięcy. Po jego upływie dokumenty są niszczone w sposób trwały – stosując procedurę niszczenia dokumentów i utylizacji nośników.

14. PROCEDURA DOSTĘPU DO POMIESZCZEŃ SZCZEGÓLNIE CHRONIONYCH

1. Pracownikom, którzy zgodnie z pełnioną funkcją lub zakresem obowiązków mają dostęp do pomieszczeń szczególnie chronionych tj. archiwum w upoważnieniu do przetwarzania danych określa się w sposób szczegółowy zakres czynności, które wykonują.
2. W rejestrze upoważnień odnotowuje się zakres udzielonego umocowania.
3. Administrator lub osoba upoważniona prowadzi rejestr wydanych kluczy dostępu do pomieszczeń szczególnie chronionych.
4. Pracownik posiadający dostęp do pomieszczeń szczególnie chronionych zobowiązany jest do:
 - a. przechowywania kluczy dostępu w sposób bezpieczny,
 - b. przebywania w pomieszczeniu bez udziału osób nieupoważnionych,
 - c. każdorazowego upewnienia się, że po opuszczeniu pomieszczenia jest ono zamknięte w sposób prawidłowy.

15. PROCEDURA PRACY NA URZĄDZENIACH PRZENOŚNYCH

Pracownik przy wykonywaniu swoich obowiązków służbowych zarówno w siedzibie administratora jak i poza nią, korzysta z urządzeń przenośnych takich jak laptop czy telefon komórkowy. Bez względu na ilość przetwarzanych za pomocą tych urządzeń danych osobowych, uwzględniając stopień ryzyka naruszenia ochrony danych osobowych, stosuje się odpowiednie zabezpieczenia tych urządzeń.

1. Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków (regulacje dotyczące komputerów przenośnych stosuje się odpowiednio do innych urządzeń przenośnych).
2. Administrator bądź wyznaczony przez niego pracownik zobowiązany jest do podejmowania działań mających na celu zabezpieczenie komputerów przenośnych poprzez:
 - a. przeprowadzenie konfiguracji oprogramowania na komputerach przenośnych, która będzie wymuszać korzystanie z haseł dostępu do urządzenia oraz okresową ich zmianę,
 - b. w przypadku braku możliwości powyższej konfiguracji oprogramowania, każdy z pracowników korzystający z urządzeń przenośnych odpowiedzialny jest we własnym zakresie za ustanowienie hasła dostępu do urządzenia oraz jego zmianę zgodnie z procedurą ustanawiania i zmiany haseł zawartą w niniejszej Polityce Bezpieczeństwa,
 - c. zabezpieczenie danych na urządzeniach przenośnych poprzez zastosowanie mechanizmu szyfrującego, który uniemożliwi zapoznanie się z danymi w razie zgubienia urządzenia,
 - d. w przypadku braku możliwości skorzystania z takiego mechanizmu, pracownik po zakończeniu wykonywania obowiązków służbowych na urządzeniach przenośnych samodzielnie szyfruje dane

(np. szyfrując pliki w których są przechowywane bądź przenosi je na zabezpieczony dysk chmurowy) w taki sposób by ich odczyt przez osoby niepowołane był niemożliwy,

- e. zainstalowanie i skonfigurowanie na komputerach przenośnych programu antywirusowego.
- f. W miarę możliwości oznaczenie każdego urządzenia przenośnego w sposób identyfikujący pracownika/pracowników korzystającego tego urządzenia,

Ponadto pracownik korzystający z urządzenia przenośnego zobowiązany jest:

1. Nie przechowywać plików prywatnych (w tym poczty prywatnej, zdjęć, dokumentów prywatnych, skanów etc.) na powierzonym sprzęcie elektronicznym tj. komputerach, telefonach, aparatach fotograficznych.
2. Zwracać szczególną uwagę na zabezpieczenie przetwarzanych danych osobowych, zwłaszcza przed dostępem do nich osób nieupoważnionych (np. poprzez wykonywanie pracy na danych w sposób uniemożliwiający podgląd danych osobom trzecim), a także przed ich zniszczeniem.
3. Nie pozostawiać urządzeń przenośnych bez nadzoru w miejscach publicznych lub samochodach. Komputery przenośne pracownik przewozi w torbach, zapewniających ich bezpieczeństwo fizyczne w razie upadku.
4. Chronić dane osobowe przechowywane na urządzeniach przenośnych przed uszkodzeniami fizycznymi, poprzez przestrzeganie zaleceń producentów dotyczących ochrony sprzętu.
5. Nie udostępniać domownikom lub innym osobom postronnym urządzeń przenośnych nawet do chwilowego korzystania.
6. Nie udostępniać domownikom lub innym osobom postronnym identyfikatora lub hasła dostępu do urządzeń przenośnych.
7. Nie korzystać z niezabezpieczonych, publicznych sieci zwłaszcza przy wykonywaniu jakichkolwiek czynności na danych osobowych.
8. Wyłączyć porty komunikacyjne (bluetooth, wi-fi itp.) w czasie kiedy nie są one wykorzystywane do pracy.
9. Przestrzegać wewnętrznych regulacji administratora dotyczących serwisowania urządzeń przenośnych oraz tworzenia kopii zapasowych danych przetwarzanych na urządzeniach przenośnych.

16. PROCEDURA PRACY NA KOMPUTERACH PRYWATNYCH

Administrator dopuszcza możliwość pracy na komputerach prywatnych przez pracownika, w tym również na korzystanie z aplikacji służących do przetwarzania danych osobowych, poza siedzibą Administratora. Procedury dotyczące korzystania ze sprzętu przenośnego administratora opisane powyżej mają odpowiednie zastosowanie w przypadku korzystania z komputerów prywatnych z tym, że pracownik w trakcie wykonywania obowiązków pracowniczych lub korzystania z aplikacji na komputerze prywatnym poza siedzibą administratora zobowiązany jest:

1. Nie pozostawiać komputerów bez nadzoru zarówno w miejscach publicznych jak i w pomieszczeniach prywatnych.
2. Utworzyć na komputerze prywatnym dodatkowe konto użytkownika w systemie operacyjnym, do którego ma dostęp wyłącznie pracownik i które będzie wykorzystywane jedynie w celu wykonywania obowiązków pracowniczych w tym dostępu do aplikacji.



3. Nie udostępniać haseł do utworzonego konta w systemie operacyjnym, służbowej poczty elektronicznej oraz aplikacji osobom trzecim, w tym innym domownikom.
4. Zabezpieczyć sprzęt komputerowy stosując zabezpieczenia takie jak antywirusy oraz kopie zapasowe, na poziomie zbliżonym do zabezpieczeń stosowanych przez administratora.

17. PROCEDURA KORZYSTANIA Z SIECI INTERNET

Niniejsza procedura dotyczy korzystania z sieci Internet podczas wykonywania obowiązków pracowniczych. Poniższe zasady mają na celu poprawę jakości i zgodności wykonywanych obowiązków służbowych z procedurami obowiązującymi w Szkole, ochronę tajemnicy służbowej, a także zabezpieczenie danych osobowych przetwarzanych w Szkole.

1. Korzystanie z sieci Internet nie może zagrażać bezpieczeństwu oprogramowania, systemu informatycznego, a także przetwarzanych danych osobowych.
2. Zabronione jest pobieranie, instalowanie oraz wykorzystywanie jakiegokolwiek oprogramowania pobranego z sieci Internet bez wiedzy i udziału osoby nadzorującej pracę w systemie informatycznym.
3. Pracownikowi zabrania się korzystania z sieci Internet w sposób, który mógłby narazić Szkołę na utratę dobrego imienia (np. otwieranie stron WWW o złej reputacji, udostępnianie chronionych informacji na portalach społecznościowych, przysyłanie pocztą elektroniczną danych osobowych bez stosownych zabezpieczeń), udostępniania łącza internetowego dostarczonego przez Szkołę osobom nieupoważnionym.
4. Zabrania się obciążania sieci Internet poprzez pobieranie aplikacji, gier, filmów, plików muzycznych, plików graficznych niezwiązanych z pełnionymi obowiązkami służbowymi.
5. Dostęp do sieci wewnętrznej oraz urządzeń zabezpieczony jest hasłem dostępu.
6. Szkoła stosuje podział oraz stopniowanie dostępu do zasobów sieci. Dopuszczalne jest także zastosowanie zablokowania dostępu do stron, które Szkoła uznaje za potencjalnie niebezpieczne.
7. W przypadku udostępniania w sieci wewnętrznej dokumentów, plików lub folderów zawierających dane osobowe konieczne jest podanie dodatkowego hasła dostępu.

18. PROCEDURA TWORZENIA ORAZ ZMIANY HASŁA

18.1. TWORZENIE HASŁA

1. Pracownicy korzystają z bezpiecznych haseł.
2. Za hasło, które nie spełnia wymogów bezpieczeństwa uznaje się hasło:
 - a. zbyt krótkie,
 - b. zawierające znaki tylko jednego rodzaju,
 - c. składające się wyłącznie lub niemal wyłącznie z nazw własnych jak np. nazwa miejscowości, imiona, marka samochodu itp.,
 - d. zawierające dane osobiste np. data urodzenia, imiona dzieci, małżonka, nr pesel, nr rejestracji samochodowej,
 - e. nie zmieniane przez długi czas (ponad 3 miesiące).



3. Pracownicy nie mogą tworzyć haseł poprzez ustalenie stałego trzonu hasła i dodawanie w kolejnym miesiącu odpowiednio cyfry 01, 02, 03 zgodnie z aktualnym miesiącem bądź samej nazwy miesiąca tj. styczeń, luty, marzec itd.
4. Hasło, z którego korzystają pracownicy powinno być hasłem złożonym z co najmniej 8 znaków i zawierać jeden z co najmniej trzech rodzajów znaków tj.:
 - a. małe litery,
 - b. wielkie litery,
 - c. cyfry,
 - d. znaki specjalne.

18.2. ZMIANA I PRZECHOWYWANIE HASŁA

1. System informatyczny automatycznie powinien wymuszać zmianę hasła nie rzadziej niż raz na 3 miesiące.
2. Osoba sprawująca nadzór nad systemem informatycznym wprowadza w systemie informatycznym oraz w aplikacjach, które służą do przetwarzania danych osobowych funkcję automatycznego wymuszania zmiany hasła przez pracownika.
3. Jeżeli brak jest możliwości ustawienia wymuszania automatycznej zmiany hasła, każdy z pracowników jest za to odpowiedzialny we własnym zakresie.
4. W przypadku podejrzenia lub stwierdzenia ujawnienia hasła, każdy z pracowników niezwłocznie zmienia hasło na nowe.
5. Hasła nie mogą być przechowywane w formie dostępnej dla osób nieupoważnionych.
6. Pracownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.
7. Pracownik utrzymuje swoje hasło w tajemnicy również po upływie jego ważności.

19. OBSŁUGA KONTA POCZTY ELEKTRONICZNEJ

1. Administrator lub wyznaczony pracownik tworzy, nadaje i odbiera dostęp do konta poczty elektronicznej.
2. Konta poczty elektronicznej tworzone są dla pracownika, zgodnie z zakresem pełnionych przez niego obowiązków służbowych.
3. W Szkole mogą być tworzone konta imienne oraz funkcyjne.
4. Dostęp do kont funkcyjnych w Szkole może posiadać kilku pracowników.
5. Dostęp do danego konta imiennego posiada wyłącznie pracownik, do którego konto jest przyporządkowane.
6. Nowo zatrudniony pracownik po przydzieleniu jednorazowego hasła zobowiązany jest do jego zmiany przy pierwszym logowaniu się do poczty elektronicznej.
7. Właścicielem wszystkich treści znajdujących się na koncie pocztowym jest Szkoła.
8. Pracownik odpowiedzialny jest za treść wysyłanych wiadomości oraz załączników.
9. Pracownik przed wysłaniem wiadomości upewnia się co do poprawności adresata.



10. Zabrania się prowadzenia korespondencji zbiorowej (wielu adresatów) wysyłanej poza Szkołę w sposób jawny dla pozostałych adresatów. W takim przypadku można wykorzystać pole adresu UDW.
11. Przed odczytaniem wiadomości elektronicznej pracownik upewnia się w pierwszej kolejności, że znany jest mu adres nadawcy.
12. Pracownik zwraca szczególną uwagę na treść i załączniki, pod kątem próby wykorzystania fałszywych podpisów, sfalszowanego adresu nadawcy, użycia nazw firm i instytucji powszechnych np. Urząd Skarbowy, DHL, Poczta Polska, Zakład Energetyczny.
13. Podejrzane wiadomości e-mail pracownik zgłasza administratorowi lub osobie nadzorującej systemem informatyczny bez wykonywania jakichkolwiek działań mogących uruchomić linki (odnośniki) w treści e-mail lub otwarcia załączników do wiadomości.
14. Zabrania się przesyłanie danych osobowych w innym celu, niż wykonywanie obowiązków służbowych.
15. Nie zaleca się korzystać z prywatnej poczty elektronicznej do realizacji celów służbowych.
16. Korzystanie ze służbowej poczty elektronicznej do celów rejestracji jakichkolwiek innych kont niezwiązanych z obowiązkami służbowymi (np. portale społecznościowe, sklepy internetowe) jest zabronione.
17. Pracownik zobowiązany jest do cyklicznej inwentaryzacji zasobów poczty elektronicznej poprzez usunięcie zbędnej korespondencji oraz jej archiwizację.

20. AKTUALIZACJA OPROGRAMOWANIA

Celem procedury jest zapewnienie ciągłości działania systemu informatycznego oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.

1. Sprzęt komputerowy oraz oprogramowanie, z którego korzystają pracownicy powinno być zgodne ze standardami obowiązującymi w Szkole w tym oprogramowanie instalowane w systemie informatycznym jest legalne.
2. Wszelkie działania związane z utrzymaniem i eksploatacją systemu informatycznego powinny być podejmowane wyłącznie przez wykwalifikowanych pracowników.
3. Wyznaczona przez administratora osoba nadzorująca systemem informatycznym dba o prawidłowe korzystanie ze sprzętu komputerowego i oprogramowania oraz zapewnia jego aktualizację.
4. Przegląd i konserwacja systemu informatycznego są wykonywane w terminach określonych przez producentów systemu jednak nie rzadziej, niż raz w roku. W miarę możliwości aktualizacja systemu informatycznego odbywa się po godzinach pracy Szkoły.
5. Osoba nadzorująca systemem informatyczny monitoruje na bieżąco pojawiające się aktualizacje i zalecenia producentów oprogramowania, z którego korzysta administrator.

21. KOPIE ZAPASOWE

Niniejsze zasady mają na celu zabezpieczenie przetwarzanych danych przed ich trwałą utratą. Szkoła zobowiązana jest wprowadzić mechanizm tworzenia kopii zapasowych danych osobowych, które przetwarza, w tym zarówno uczniów ich rodziców i opiekunów prawnych jak i nauczycieli i pracowników Szkoły. W tym celu wprowadza się następującą procedurę:

1. Przez kopię zapasową rozumie się kopię (roboczą) wykonywaną po każdym dniu pracy lub po zamknięciu jakiegoś etapu pracy. Kopiowaniu podlegają wyłącznie pliki, na których pracownik wykonywał zmiany.
2. Kopia bezpieczeństwa – jest kopią systemową, sporządzaną rzadziej ale obejmuje ona wszystkie pliki, katalogi oraz systemy, w których pracownik przetwarza dane osobowe.
3. Osoba nadzorująca system informatyczny w Szkole wspólnie z administratorem ustala częstotliwość sporządzania kopii zapasowych, bezpieczeństwa oraz ich ilość.
4. Osoba nadzorująca system informatyczny wprowadza w oprogramowaniu serwera zmiany, po których kopia wykonywana jest automatycznie w oparciu o zaplanowany interwał czasowy.
5. Jeśli oprogramowanie serwera/dysku sieciowego uniemożliwia ustawienie polecenia automatycznego wykonywania kopii zapasowych, osoba nadzorująca system informatyczny w Szkole wykonuje kopię zapasową w sposób ręczny.
6. Kopie zapasowe zapisuje się na: (należy wybrać stosowane formy)
 - a. dyskach zainstalowanych na serwerze, z którego kopia została wykonana,
 - b. dysku chmurowym,
7. Pracownik odpowiada indywidualnie za sporządzanie kopii zapasowych z urządzenia końcowego, na którym wykonuje swoją pracę.
8. Zabrania się wykonywania kopii zapasowych z urządzeń końcowych na nośniki nie będące własnością administratora bez konsultacji z administratorem lub osobą nadzorującą system informatyczny.
9. Kopie zapasowe podlegają okresowemu przeglądowi pod kątem ich wydajności i przydatności.
10. Kopie, które straciły swą przydatność dla Szkoły, należy usunąć zgodnie z procedurą archiwizacji.
11. Zabrania się wyrzucania do śmietnika nośników danych, na których zapisane były kopie zapasowe.

22. ARCHIWIZACJA

1. Administrator lub wyznaczony pracownik odpowiada za przeprowadzenie archiwizowania akt dokumentów, danych, poczty, faktur i innych dokumentów księgowych oraz finansowych w przyjętych ramach czasowych.
2. Dokumenty podlegające archiwizacji umieszczane są w opisanych segregatorach lub teczkach.
3. Administrator w miarę możliwości powinien wyznaczyć pomieszczenie przeznaczone na archiwum.
4. Pomieszczenie archiwum, stanowi obszar przetwarzania danych osobowych i jest pomieszczeniem szczególnie chronionym w Szkole.



5. Pomieszczenie archiwum powinno być wyposażone w środki bezpieczeństwa fizycznego podnoszące bezpieczeństwo przechowywanych tam dokumentów przynajmniej o jeden poziom wyżej, niż pozostałe pomieszczenia będące obszarem przetwarzania.
6. Za środki bezpieczeństwa fizycznego podnoszące poziom bezpieczeństwa uznaje się:
 - a. pomieszczenie znajdujące się na innej kondygnacji niż 0,
 - b. pomieszczenie bez okna,
 - c. pomieszczenie w oknach którego znajduje się kratka lub roleta antywłamaniowa,
 - d. pomieszczenie do którego zastosowano drzwi antywłamaniowe i ogniotrwałe,
 - e. zastosowano system alarmowy,
 - f. zainstalowano zamek magnetyczny otwierany indywidualnymi kartami lub kodami,
 - g. zainstalowano dodatkową kamerę monitoringu wizyjnego skierowaną na drzwi wejściowe,
 - h. pomieszczenie archiwum wyposażono w higrometr i termometr.
7. Zabrania się umieszczania dokumentacji bezpośrednio na podłodze.
8. W przypadku kiedy Szkoła nie dysponuje warunkami lokalowymi umożliwiającymi wydzielenie pomieszczenia archiwum, administrator powinien przeznaczyć przynajmniej jedną szafę metalową/sejf na dokumenty archiwalne.

23. KONSERWACJA I NAPRAWA SPRZĘTU

Administrator stosując się do ogólnych zasad przetwarzania danych osobowych, w tym w szczególności do zapewnienia ochrony danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabranianiem przez osobę nieuprawnioną oraz zmianą, utratą, uszkodzeniem lub zniszczeniem ma obowiązek zabezpieczenia danych przy udostępnianiu sprzętu lub dostępu do obszarów przetwarzania osobom trzecim. Wobec tego administrator wprowadza następujące reguły postępowania:

1. W przypadku wykonywania prac remontowych, montażowych bądź naprawczych (w tym również sprzętu komputerowego) przez podmioty zewnętrzne, dane osobowe zostają należycie zabezpieczone przed nieupoważnionym dostępem.
2. Ryzyko utraty bezpieczeństwa danych osobowych przetwarzanych przez administratora pojawiające się ze strony osób trzecich, które mają do nich dostęp (typu bieżąca konserwacja i naprawy wykonywane przez firmy zewnętrzne), jest zabezpieczone poprzez podpisanie umów powierzenia przetwarzania danych osobowych.
3. Umowa powierzenia danych osobowych jest zawierana przed przystąpieniem przez podmiot zewnętrzny do wykonywanych czynności.
4. Jeśli jest to konieczne dopuszcza się konserwowanie oraz naprawę sprzętu poza siedzibą Szkoły jedynie po jego zabezpieczeniu. Przed przekazaniem uszkodzonego sprzętu, wykonuje się kopię zapasową danych oraz stosuje się przynajmniej jedną z poniższych czynności:
 - a. wymontowanie nośników z danymi jeśli to możliwe,
 - b. trwałe usunięcie danych,
 - c. szyfrowanie danych.
5. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w protokołach podpisywanych przez osoby w tych działaniach uczestniczące.



6. Doraźne czynności konserwacyjne i naprawcze wykonywane bez zawarcia umowy o powierzeniu danych osobowych muszą być przeprowadzane pod stałym nadzorem pracowników. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych, jest zabezpieczane poprzez zobowiązanie ich do zachowania tajemnicy na podstawie pisemnych oświadczeń.

24. NISZCZENIE DOKUMENTÓW I UTYLIZACJA NOŚNIKÓW

Niniejsza procedura utylizacji dotyczy zarówno nośników w formie papierowej, jak i elektronicznej.

1. Nośniki przeznaczone do zniszczenia przechowywane są w wydzielonym i zabezpieczonym miejscu.
2. Dokumenty papierowe zawierające dane osobowe, niszczone są w niszczarce, w sposób uniemożliwiający ich odczytanie.
3. Wycofane z użytku nośniki elektroniczne (uszkodzone, wyeksploatowane) przeznaczone do utylizacji pozbawia się wcześniej zapisu danych lub w sposób mechaniczny pozbawia się możliwości ich odczytu.
4. Poprzez trwałe usunięcie danych rozumie się wykorzystanie specjalistycznego oprogramowania, uniemożliwiającego odtworzenie danych.
5. Pracownik niszczy dokumentację papierową samodzielnie, a niepotrzebne lub uszkodzone nośniki elektroniczne przekazuje administratorowi lub wyznaczonemu pracownikowi.
6. Utylizacja nośników elektronicznych odbywa się po uzyskaniu zgody administratora i zostaje potwierdzona protokołem zniszczenia.
7. Wzór protokołu zniszczenia ustala administrator. Protokół powinien zawierać w szczególności datę, przyczynę zniszczenia nośników oraz podpisy osób uprawnionych do zniszczenia nośników.
8. W przypadku korzystania z usług zewnętrznego podmiotu utylizującego dokumentację zawierającą dane osobowe niezbędne jest uprzednie zawarcie umowy powierzenia danych osobowych. Administrator lub wyznaczony pracownik zobowiązany jest do odebrania protokołu zniszczenia wystawionego przez podmiot zewnętrzny.

25. UTRZYMANIE CZYSTOŚCI

Pomieszczenia, w których znajdują się dane osobowe zarówno w postaci papierowej jak i elektronicznej, które przechowywane są na stacjach komputerowych bądź innych urządzeniach umożliwiających dostęp do danych, stanowią obszar przetwarzania danych osobowych. Dostęp do tych obszarów powinien być kontrolowany zwłaszcza w zakresie w jakim jest on udostępniany osobom sprzątającym. Niezależnie od tego czy osoby sprzątające pomieszczenia, w których przetwarza się dane osobowe są zatrudnione wewnątrz struktury organizacyjnej administratora czy są to osoby świadczące usługi z zewnątrz, administrator wprowadza następujące reguły:

1. Wszystkie osoby sprzątające zobowiązane są do zachowania w tajemnicy danych osobowych znajdujących się w obszarze przetwarzania danych osobowych podczas wykonywania czynności.
2. Oświadczenie o zachowaniu w tajemnicy powinno być odbierane przez administratora przed przystąpieniem osoby sprzątającej do wykonywania czynności.
3. Oświadczenie o zachowaniu w tajemnicy danych osobowych może stanowić oddzielny dokument bądź zostać zawarte w treści umowy o pracę bądź innej podstawy świadczenia usług.



4. Przed rozpoczęciem sprzątania pracownicy zobowiązani są zastosować się do zasady czystego biurka oraz zasady czystego ekranu oraz umożliwić wejście i rozpoczęcie wykonywanych czynności przez osobę sprzątającą.
5. Osoby sprzątające pomieszczenia, w których przetwarzane są dane osobowe powinny wykonywać czynności sprzątania pod nadzorem i w obecności pracowników.
6. W przypadku realizacji usług bez nadzoru pracownika, pracownik zobowiązany jest do zabezpieczenia obszaru przetwarzania poprzez umieszczenie dokumentacji/nośników w szafkach zamykanych na klucz oraz wylogowania z systemu informatycznego.
7. Powyższe zasady mają również zastosowanie do innych osób świadczących usługi np. remontowe, serwisowe.

26. PROCEDURA POSTĘPOWANIA W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Celem procedury jest określenie ogólnych zasad postępowania w przypadku naruszenia bezpieczeństwa danych osobowych przetwarzanych zarówno tradycyjnie, jak również w systemie informatycznym w Szkole. Niniejsza procedura zapewnia, że zdarzenia związane z bezpieczeństwem danych oraz zagrożenia związane z funkcjonowaniem systemu informatycznego, zgłaszane są w sposób umożliwiający niezwłoczne podjęcie działań naprawczych oraz eliminację negatywnych skutków związanych z zaistniałym incydem.

Zasady postępowania w przypadku naruszenia ochrony danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych.

Reakcja na incydent zależy od jego istotności, mierzonej skutkami i poziomem oddziaływania na Szkołę lub na osoby, których dane osobowe były objęte incydem.

Osoby stwierdzające naruszenie zasad ochrony lub zdarzenie, które mogło skutkować takim naruszeniem, zobowiązane są do przestrzegania oraz postępowania według opracowanej i wdrożonej procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

26.1. ISTOTA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do:

- a. "naruszenia poufności" – polegającego na nieuprawnionym lub przypadkowym ujawnieniu lub udostępnieniu danych osobowych,
- b. "naruszenia integralności" – polegającego na nieuprawnionym lub przypadkowym zmodyfikowaniu danych osobowych,
- c. "naruszenia dostępności" – polegającego na przypadkowej lub nieuprawnionej utracie dostępu do danych osobowych lub ich zniszczeniu.

Naruszeniem danych osobowych jest przede wszystkim każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną czy uszkodzenia jakiegokolwiek elementu systemu informatycznego.

Obowiązek zgłoszenia jest wymagany, przede wszystkim w sytuacji, gdy naruszenie polegało na:

1. Zgubieniu lub kradzieży nośnika/urządzenia.
2. Zgubieniu, kradzieży lub pozostawieniu w niebezpiecznej lokalizacji dokumentacji papierowej zawierającej dane osobowe.
3. Utracie korespondencji papierowej przez operatora pocztowego lub otwarcie przed zwróceniem jej do nadawcy.
4. Nieuprawnionym uzyskaniu dostępu do informacji.
5. Nieuprawnionym uzyskaniu dostępu do informacji poprzez złamanie zabezpieczeń.
6. Ingerencji złośliwego oprogramowania ingerującego w poufność, integralność i dostępność danych.
7. Uzyskaniu poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail, czy też inny komunikator internetowy.
8. Nieprawidłowej anonimizacji danych osobowych w dokumencie.
9. Nieprawidłowym usunięciu/zniszczeniu danych osobowych z nośnika/ urządzenia elektronicznego przed jego zbyciem przez administratora.
10. Niezamierzonej publikacji.
11. Przesłaniu danych osobowych do niewłaściwego odbiorcy.
12. Ujawnieniu danych niewłaściwej osobie.
13. Ustnym ujawnieniu danych osobowych.

26.2. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.
2. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz powiadomić odpowiednie organy/służby ochrony oraz bezpośredniego przełożonego.
3. Z każdego zdarzenia pracownik sporządza notatkę i przekazuje ją administratorowi. W notatce należy ująć:
 - a. datę i miejsce stwierdzenia naruszenia,
 - b. sposób stwierdzenia naruszenia (opis sytuacji),
 - c. podjęte działania (wykonane czynności po wykryciu naruszenia),
 - d. wskazanie osób poinformowanych o zaistniałym incydencie,
 - e. czytelny podpis osoby sporządzającej notatkę.
4. Po przedłożeniu notatki z naruszenia administrator lub wyznaczona przez niego osoba informuje inspektora o zaistniałym zdarzeniu oraz dokonuje jego analizy.
5. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, administrator lub osoba przez niego wyznaczona dokonuje oceny istotności naruszenia.
6. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:



- a. charakter naruszenia ochrony danych osobowych (naruszenie poufności, integralności, dostępności),
 - b. klasyfikacja naruszenia (na czym polegało naruszenie),
 - c. przyczyny naruszenia (wewnętrzne działanie niezamierzone/zamierzone, zewnętrzne działanie niezamierzone/zamierzone),
 - d. kategorie danych osobowych i przybliżoną liczbę osób, których dane dotyczą,
 - e. kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
 - f. środki bezpieczeństwa zastosowane przed naruszeniem,
 - g. możliwe konsekwencje naruszenia ochrony danych osobowych (naruszenie praw lub wolności osób fizycznych),
 - h. wpływ incydentu na ciągłość działania Szkoły,
 - i. koszty usunięcia skutków incydentu,
 - j. szacowany czas naprawy skutków wywołanych incydem.
7. Ocena istotności naruszenia prowadzi do zakwalifikowania incydentu według przyjętej skali:
- a. pomijalne,
 - b. niskie,
 - c. akceptowalne,
 - d. wysokie,
 - e. maksymalne.
8. W celu dokonania zgłoszenia administrator stosuje formularz udostępniony przez Urząd Ochrony Danych Osobowych.
9. Inspektor dokumentuje zaistniały przypadek naruszenia oraz sporządza raport.
10. Zgłoszenie incydentu rejestrowane jest przez administratora lub wyznaczoną przez niego osobę w rejestrze incydentów.

26.3. KONSEKWENCJE ZANIECHANIA ZGŁOSZENIA NARUSZENIA OCHRONY DANYCH

1. Wobec pracownika, który w przypadku naruszenia danych osobowych nie podjął działania określonego w niniejszym dokumencie, a w szczególności nie powiadomił administratora lub odpowiedniej osoby, zgodnie z określonymi zasadami może zostać wszczęte postępowanie dyscyplinarne lub porządkowe.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.
3. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia administratora o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej oraz cywilnej zgodnie z obowiązującymi przepisami.

26.4. UDOKUMENTOWANIE SKUTKÓW ORAZ PODJĘTYCH ŚRODKÓW I DZIAŁAŃ

Pracownik, który stwierdził fakt lub uzyskał informację o naruszeniu bezpieczeństwa danych osobowych jest obowiązany niezwłocznie powiadomić administratora i/lub inspektora oraz osobę nadzorującą system informatyczny. Administrator lub osoba przez niego wyznaczona mają obowiązek:

1. Wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i godziną oraz podpisać.
2. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby nieuprawnionej do danych osobowych w systemie informatycznym służącym do przetwarzania danych osobowych.
3. Podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem śladów naruszenia ochrony, w szczególności poprzez:
 - a. fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie nieuprawnionej,
 - b. wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
 - c. zmianę hasła użytkownika, przez konto którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu.
4. Dokonać szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia bezpieczeństwa danych osobowych.
5. Przywrócić prawidłowe działanie systemu informatycznego służącego przetwarzaniu danych osobowych.
6. Po przywróceniu prawidłowego stanu, należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podjąć kroki, mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
7. Jeżeli przyczyną zdarzenia był błąd pracownika, należy przeprowadzić szkolenie dotyczące bezpieczeństwa przetwarzania danych osobowych w Szkole.
8. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym szkodliwym oprogramowaniem, należy ustalić źródło jego pochodzenia i utworzyć zabezpieczenia antywirusowe oraz organizacyjne, wykluczające podobne zdarzenia w przyszłości.

26.5. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędowi Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
 - a. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
 - b. zawierać imię i nazwisko oraz dane kontaktowe inspektora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
 - c. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
 - d. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania niniejszego artykułu.

26.6. ZAWIADAMIANIE 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, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
 - a. administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym tych danych osobowych,
 - b. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1,
 - c. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

27. POSTANOWIENIA KOŃCOWE

1. Administrator zobowiązany jest zapoznać z dokumentem wszystkie osoby przetwarzające dane osobowe.
2. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce Bezpieczeństwa może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
3. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy RODO oraz przepisy Ustawy.
4. Pracownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Bezpieczeństwa. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w Szkole pracownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.
5. W sprawach nieokreślonych w niniejszym dokumencie należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.



6. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą Polityką Bezpieczeństwa oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
7. Polityka wchodzi w życie z dniem podpisania.

Załączniki:

1. **Załącznik nr 1** - Oświadczenie pracownika
2. **Załącznik nr 2** - Upoważnienie pracownika
3. **Załącznik nr 3** - Wzór rejestru upoważnień
4. **Załącznik nr 4** - Klauzula informacyjna
5. **Załącznik nr 5** - Klauzula informacyjna dla pracowników
6. **Załącznik nr 6** - Klauzula informacyjna dla kandydatów do pracy
7. **Załącznik nr 7** - Wzór umowy powierzenia danych osobowych
8. **Załącznik nr 8** - Wzór rejestru umów powierzenia
9. **Załącznik nr 9** - Procedura realizacji praw osób fizycznych

Dokument sporządzono:	Opracował	Sprawdził	Zatwierdził (ADO)
Data:			
Miejsce:			



PLAN SPRAWDZEŃ: Data	Sprawdził (AW lub IOD)	Zatwierdził (ADO)
.....2019 r.		
.....2020 r.		
.....2021 r.		
.....2022 r.		

