POLITYKA
OCHRONY DANYCH
I LICEUM OGÓLNOKSZTAŁCĄCEGO
IM. ADAMA MICKIEWICZA W SULĘCINIE

SPIS TREŚCI:

I. WSTĘP

1. Celem Polityki ochrony danych osobowych, zwanej dalej Polityką, jest wprowadzenie i utrzymanie wymaganej przez przepisy rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000) właściwej ochrony danych osobowych w związku z przetwarzaniem danych osobowych w I Liceum Ogólnokształcącym im. Adama Mickiewicza w Sulęcinie.
2. Polityka ochrony danych została wdrożona Zarządzeniem Dyrektora I Liceum Ogólnokształcącego im. Adama Mickiewicza w Sulęcinie nr 31/2021/2022.
3. Niniejsza Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych. Dotyczy istniejących oraz przetwarzanych w przyszłości zbiorów danych osobowych. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów, stażystów.
4. Niniejszy dokument opisuje sposoby przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

II. PODSTAWOWE POJĘCIA

- **Liceum** – w tym dokumencie jest rozumiane jako I Liceum Ogólnokształcące im. Adama Mickiewicza w Sulęcinie, zlokalizowane przy ulicy E. Plater 1; 69-200 Sulęcin,
- **Administrator danych** (ADO) – I Liceum Ogólnokształcące im. Adama Mickiewicza w Sulęcinie, reprezentowane przez Dyrektora Liceum,
- **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
- **Przetwarzanie danych osobowych** – gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
- **System informatyczny** – system (urządzenia, narzędzia, programy), w których przetwarzane są dane osobowe,
- **Zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.
- **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,
- **Ustawa o ochronie danych osobowych** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000),
- **Polityka** – w tym dokumencie jest rozumiana jako Polityka ochrony danych obowiązująca w I Liceum Ogólnokształcącym im. Adama Mickiewicza,
- **Inspektor ochrony danych** – osoba wyznaczona przez Administratora Danych do nadzorowania przestrzegania zasad ochrony danych osobowych oraz przygotowania dokumentów wymaganych przez obowiązujące przepisy w I Liceum Ogólnokształcącym im. Adama Mickiewicza w Sulęcinie,
- **Użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w Liceum, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Liceum.
- **Identyfikator użytkownika** – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- **Administrator Systemu Informatycznego (ASI)** – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie,
- **Sieć lokalna** – połączenie komputerów pracujących w Liceum w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych;
- **Sieć publiczna** – sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy Prawo telekomunikacyjne,
- **Sieć telekomunikacyjna** – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy Prawo telekomunikacyjne,
- **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

- **Przetwarzanie danych** – rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
- **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
- **Teletransmisja** – przesyłanie informacji za pomocą sieci telekomunikacyjnej,
- **Aplikacja** – program komputerowy wykonujący konkretne zadanie.

III. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

Polityka ochrony danych opisuje zasady i procedury gromadzenia, przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz szkoły. Odnosi się całościowo do problemu zabezpieczenia danych osobowych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

IV. WYKAZ BUDYNKÓW I POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

LP.	ADRES-BUDYNEK	POMIESZCZENIA
1.	Budynek I LO ul. Emilii Plater 1 69-200 Sulęcin	gabinet dyrektora sekretariat księgowość gabinet pedagoga i psychologa szkolnego pokój nauczycielski sale lekcyjne

V. ZBIORY DANYCH PRZETWARZANYCH W SYSTEMACH INFORMATYCZNYCH I OPIS STRUKTUR PRZETWARZANYCH DANYCH OSOBOWYCH

ZBIÓR DANYCH OSOBOWYCH	PROGRAM INFORMATYCNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Pracownicy	QNT Kadry	PESEL/ NIP/ imię (imiona) i nazwisko/ poprzednie nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres stały/ numer telefonu/ e-mail/ dowód osobisty (seria i nr., wydany przez, data wydania)/ imię ojca/ imię matki/ nazwisko panieńskie matki/ stan cywilny i rodzinny/ nr legitymacji służbowej/ emeryt/ rencista/ obywatelstwo/ osoba kontaktowa/ wykształcenie/ nazwa szkoły i rok ukończenia/ warunki zatrudnienia/ awans zawodowy/ staż pracy/ warunki zatrudnienia/ wysokość wynagrodzenia/ ukończone kursy/ kary i nagrody/ tytuł zawodowy/ nieobecności w pracy/ informacja o badaniach i stanie zdrowia/
	PŁATNIK	PESEL/ NIP/ imię i nazwisko/ adres/ data i miejsce urodzenia
	QNT Płace Vulcan Płace	PESEL/ NIP/ imię (imiona) i nazwisko/ poprzednie nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres stały/ numer telefonu/ e-mail/ dowód osobisty (seria i nr., wydany przez, data wydania)/ imię ojca/ imię matki/ stan cywilny i rodzinny/ nr legitymacji służbowej/ emeryt/ rencista/ obywatelstwo/ posiada gospodarstwo rolne/ wykształcenie/ nazwa szkoły i rok ukończenia/ warunki zatrudnienia/ awans zawodowy/ staż pracy/ warunki zatrudnienia/ wysokość wynagrodzenia/ ukończone kursy/ kary i nagrody/ tytuł zawodowy/ nieobecności w pracy
	QNT Księgowość	PESEL/ NIP/ imię/ nazwisko/ adres/ data i miejsce urodzenia/ numer konta bankowego
	QNT Środki Trwałe	imię/ nazwisko
Nauczyciele/ Uczniowie	SIO	PESEL/ imię/ nazwisko/ płeć/ obywatelstwo/ stopień awansu zawodowego/ wykształcenie/ kwalifikacje/ tytuł zawodowy/ warunki zatrudnienia/ nieobecności/ staż pracy/ wynagrodzenie/ uprawnienia/ pomoc materialna/
	LIBRUS E-Dziennik Plan Lekcji	PESEL/ imię i nazwisko/ data i miejsce urodzenia/ płeć/ adres/ nr telefonu/ imiona i nazwiska rodziców/ adresy rodziców (opiekunów prawnych)/ nr legitymacji/ informacje o wynikach w nauce/ informacja o nieobecnościach

Uczniowie	LIBRUS Świadectwa	PESEL/ imię i nazwisko/ data i miejsce urodzenia/ informacje o wynikach w nauce/
Nauczyciele/Uczniowie	G-Suite for Schools	imię i nazwisko/ adres e-mail/ tworzone i przesyłane dokumenty wewnętrzne/ informacje o wynikach w nauce

VI. ZBIORY DANYCH PRZETWARZANYCH TRADYCYJNIE

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA SŁUŻĄCA DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Pracownicy	Akta Osobowe	PESEL/ imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres stały/ nr telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imię ojca/ imię matki/ stan cywilny i rodzinny/ stosunek do służby wojskowej/ nr legitymacji służbowej/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo/ osoba kontaktowa/ wykształcenie/ warunki zatrudnienia/ wynagrodzenie/ nr konta/ staż pracy/ historia pracy/ kary/ nagrody/ tytuł zawodowy/ kwalifikacje/ nieobecności/ kursy/ badania/ informacje o stanie zdrowia/ stopień awansu zawodowego/
	Orzeczenia lekarskie do celów sanitarno-epidemiologicznych	PESEL/ imię i nazwisko/ adres stały/ informacje o stanie zdrowia
	Oświadczenia i wnioski do Funduszu Socjalnego	imię i nazwisko/ adres stały/ wysokość zarobków/
	Listy Płac/ Fundusz Płac	PESEL/ imię i nazwisko/ stanowisko/ wynagrodzenie
	Karty zasiłkowe	PESEL/ NIP/ imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ adres stały/ okresy niezdolności do pracy/ stanowisko
	Karty zarobkowe	PESEL/ NIP/ imię i nazwisko/ nazwisko rodowe/ wysokość zarobków/ warunki zatrudnienia/
	PIT-y	PESEL/ NIP/ imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ adres/ wysokość zarobków
	Zaświadczenia	PESEL/ NIP/ imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ adres/ wysokość zarobków/ warunki pracy/
	Dokumentacja ubezpieczeniowa (ZUS)	PESEL/ imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ adres stały/ informacja o stanie zdrowia/ okresy niezdolności do pracy
	Arkusz Organizacyjny	imię i nazwisko/ staż pracy/ tytuł zawodowy/ stopień awansu zawodowego/ kursy/ kwalifikacje/ zawód wyuczony/ warunki zatrudnienia/

		nieobecności/ informacja o postępowaniu kwalifikacyjnym/ informacja o zwolnieniach
	Dokumentacja awansów zawodowych nauczycieli	imię i nazwisko/ data i miejsce urodzenia/ adres stały/ wykształcenie/ historia pracy/ kwalifikacje
	Ewidencja pracowników	imię i nazwisko/ nazwisko rodowe/ data urodzenia/ stanowisko/ adres/ data zatrudnienia i zwolnienia
	Szkolenia BHP	imię i nazwisko/ data zatrudnienia/ stanowisko
	Ewidencja delegacji	imię i nazwisko/
	Rejestr zwolnień lekarskich	imię i nazwisko/ okres niezdolności do pracy
	Kandydaci do pracy	podania/kwestionariusze imię i nazwisko/ imiona rodziców/ data urodzenia/ obywatelstwo/ adres/ wykształcenie/ historia zatrudnienia/ kwalifikacje i umiejętności/ / dowód osobisty
	Praktykanci/ Stażyści	umowy/podania imię i nazwisko/ PESEL/ data i miejsce urodzenia/ adres/ wykształcenie/nr telefonu
Uczniowie	Dokumentacja uczniów	PESEL/ imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres/ nr telefonu/ mail/ dowód osobisty/ imiona i nazwiska rodziców (opiekunów prawnych)/ adresy rodziców (opiekunów)/ stan cywilny/ nr legitymacji/ obywatelstwo/ osoba kontaktowa/ wykształcenie/ historia nauki/ wyznanie/ informacje o stanie zdrowia
	Księga Uczniów	PESEL/ imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ adres/ imiona i nazwiska rodziców (opiekunów prawnych)
	Dzienniki lekcyjne	PESEL/ imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres/ nr telefonu/ dowód osobisty/ imiona i nazwiska rodziców (opiekunów prawnych)/ adresy i nr tel. rodziców (opiekunów)/ stan cywilny/ obywatelstwo/ nieobecności/ informacje o wynikach w nauce/
	Księga wydanych legitymacji	imiona/ nazwisko/ data urodzenia/ adres/ numer legitymacji
	Rejestr Zaświadczeń	imię i nazwisko/ data i miejsce urodzenia/ adres/
	Księga absolwentów	imię i nazwisko/ data ukończenia szkoły
	Świadectwa, duplikaty, rejestr wydanych świadectw	PESEL/ imię i nazwisko/ data i miejsce urodzenia/ informacja o wynikach w nauce/ nr świadectwa
	Dokumentacja ubezpieczeniowa (protokoły powypadkowe, rejestr wypadków)	imię i nazwisko/ PESEL/ data urodzenia/ dowód osobisty/ adres/ nr telefonu/

	Karta zdrowia uczniów	PESEL/ imię i nazwisko/ data i miejsce urodzenia/ adres/ imiona i nazwiska rodziców/ Informacje o stanie zdrowia
	Rejestr wydanych opinii PPP	imię i nazwisko/ data urodzenia/ adres/ diagnoza psychologiczno-pedagogiczna
	Stypendyści	imię i nazwisko/ adres/ PESEL/ data i miejsce urodzenia/ dochód/ telefon/ imiona i nazwiska rodziców (opiekunów prawnych)/ informacja o pomocy socjalnej/ informacja o wynikach w nauce
Kandydaci do liceum	podania do liceum wraz z załącznikami	imię i nazwisko/ PESEL/ data i miejsce urodzenia/ adres/ nr tel./ imiona i nazwiska rodziców (opiekunów prawnych)/ adres i nr telefonu rodziców (opiekunów prawnych)/ historia nauki/ wyniki nauczania w gimnazjum

VII. SPOSÓB PRZEPŁYWU DANYCH OSOBOWYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

1. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
2. Przesyłanie danych pomiędzy systemami i programami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. CD, DVD, dysk wymienny, PenDrive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu/importu danych za pomocą teletransmisji.
3. Przesyłanie danych może odbywać się zarówno w obrębie szkoły, jak i na zewnątrz (do organu prowadzącego szkołę lub podmiotów współpracujących ze szkołą w organizowaniu zadań związanych z procesem edukacyjnym, w szczególności organizujących egzamin maturalny –OKE i CKE (dane uczniów: nazwisko, imiona, data i miejsce urodzenia, PESEL).
4. Dane osobowe przetwarzane w Liceum za pomocą opisanego oprogramowania przesyłane są pomiędzy poszczególnymi programami w następujący sposób:

a. E- dziennik przesyła dane do programu E-Świadectwa.
b. System QNT – Dane z programu kadrowego zostają przesłane do programu płacowego i odwrotnie.
c. Program Płatnik przesyła zaszyfrowane deklaracje rozliczeniowe do ZUS.
d. Program SIO wykorzystuje wygenerowane dane z dostępnych systemów i przygotowuje raport zbiorczy dla jednostki nadrzędnej.
e. Internet Banking - generuje dane, które są przesyłane do Banku Spółdzielczego w Ośnie Lubuskim oddział Sulęcin

VIII. ŚRODKI TECHNICZNE I ORGANIZACYJNE STOSOWANE W PRZETWARZANIU DANYCH

Zasady przetwarzania danych osobowych

Administrator danych przetwarza dane osobowe:

- zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
- zbiera je w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami („ograniczenie celu");
- adekwatnie, stosownie oraz w sposób ograniczony do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
- prawidłowo i w razie potrzeby uaktualnia zebrane dane („prawidłowość");
- przechowuje je w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; („ograniczenie przechowywania");
- w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

W celu realizacji tych zasad administrator danych przetwarza dane legalnie, na podstawie przesłanek opisanych w art. 6 i art. 9 RODO. Pobiera dane osobowe adekwatnie do celów przetwarzania i przetwarza je przez określony czas. Wobec osób, których dane przetwarza wypełnia obowiązki informacyjne określone w art. 13 RODO lub w art. 14 RODO (gdy informacje pobierane są w sposób inny niż od osoby, której dane dotyczą) oraz wskazuje przysługujące im uprawnienia takie jak prawo do:

- dostępu do danych,
- sprostowania danych,
- usunięcia danych (prawo do bycia zapomnianym),
- przenoszenia,
- sprzeciwu wobec przetwarzania,
- ograniczenia przetwarzania,
- wniesienia skargi do organu nadzorczego
- sprzeciwu wobec bycia profilowanym.

Administrator danych zapewnia ochronę danych w przypadku korzystania z usług podmiotów zewnętrznych, w postaci zawierania stosownych umów powierzenia oraz korzystając z usług podmiotów przetwarzających realizujących obowiązki wynikające z RODO. W razie wystąpienia incydentu technicznego lub fizycznego administrator danych zapewnia zdolność do szybkiego przywrócenia dostępności do danych osobowych i dostępu do nich.

Potwierdzenie spełniania obowiązków informacyjnych przez administratora danych stanowią, klauzule informacyjne przekazywane osobom, których dane są przetwarzane. W przypadku pracowników przedstawia się im klauzule do podpisania i zamieszcza w ich aktach osobowych. W przypadku uczniów i ich rodziców/opiekunów prawnych klauzule wywieszone są na tablicach informacyjnych znajdujących się na korytarzu Liceum oraz zamieszczone są na stronie internetowej Liceum.

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, stosuje się wysoki poziom bezpieczeństwa. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

Administrator danych zapewnia, aby dostęp do danych osobowych w Liceum miały tylko osoby legitymujące się nadanym przez ADO upoważnieniem. Upoważnienia określają do jakich operacji użytkownicy są uprawnieni tj. tworzenia, usuwania, wglądu, przekazywania danych, w jakich systemach oraz na jaki czas. Administrator danych prowadzi ewidencję osób upoważnionych. Upoważnienia do przetwarzania danych osobowych mogą być nadawane na wniosek bezpośredniego przełożonego użytkownika systemu.

Udostępnianie i powierzanie danych osobowych

1. Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.
2. Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy

a. adresat wniosku (administrator danych),
b. wnioskodawca,
c. podstawa prawna (wskazanie potrzeby),
d. wskazanie przeznaczenia,
e. zakres informacji.

3. Administrator odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

2. Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

Stosowane środki ochrony zabezpieczenia

FORMA PRZETWARZANIA DANYCH	STOSOWANE ŚRODKI OCHRONY
dane przetwarzane w sposób tradycyjny	– przechowywanie danych w pomieszczeniach zamykanych na zamki patentowe; – przechowywanie danych osobowych w szafach zamykanych na klucz; – zastosowanie czujników ruchu informujących o nieautoryzowanym wejściu do budynku; – zastosowanie monitoringu wizyjnego; – przetwarzanie danych wyłącznie przez osoby posiadających upoważnienie nadane przez ABI; – zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania;
dane przetwarzane w systemach informatycznych	– kontrola dostępu do systemów; – zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony; – stosowanie ochrony zasilania; – systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; – składowanie danych sensytywnych oraz nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach;

	– zabezpieczenie pomieszczenia serwerowni; – przydzielenie pracownikom indywidualnych kont użytkowników i haseł; – stosowanie indywidualnych haseł logowania do poszczególnych programów; – właściwa budowa hasła;

IX. ANALIZA RYZYKA ZWIĄZANEGO Z PRZETWARZANIEM DANYCH OSOBOWYCH

Administrator danych prowadzi analizę ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń. Analiza prowadzona jest w przypadku zaistnienia zagrożenia oraz cyklicznie raz w roku. Analiza danych prowadzona jest osobno dla każdego zbioru danych lub dla kilku zbiorów o podobnym zakresie danych. W przypadku konieczności przeprowadza się ocenę skutków dla oceny ryzyka na mocy art. 35 RODO.

Szczegółowy sposób prowadzenia analizy ryzyka zawiera Procedura analizy ryzyka, stanowiąca odrębny dokument. Przygotowano również aktualizowany Wykaz zagrożeń.

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
dane przetwarzane w sposób tradycyjny	– oszustwo, kradzież, sabotaż; – zdarzenia losowe (powódź, pożar); – zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); – niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; – pokonanie zabezpieczeń fizycznych; – podsłuchy, podglądy; – ataki terrorystyczne; – brak rejestrowania udostępniania danych; – niewłaściwe miejsce i sposób przechowywania dokumentacji;
dane przetwarzane w systemach informatycznych	–nie przydzielenie użytkownikom systemu informatycznego identyfikatorów; –niewłaściwa administracja systemem; –niewłaściwa konfiguracja systemu; –zniszczenie (sfałszowanie) kont użytkowników; –kradzież danych kont; –pokonanie zabezpieczeń programowych; –zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); –niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; - zdarzenia losowe (powódź, pożar); - niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych; -naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione;

	- przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznej lub sieci; -przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci; - przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych; - brak rejestrowania zdarzeń tworzenia lub modyfikowania danych;

X. REJESTR CZYNNOŚCI PRZETWARZANIA

Administrator danych prowadzi rejestr czynności przetwarzania. W rejestrze tym zamieszcza:

a) imię i nazwisko oraz dane kontaktowe administratora;

b) cele przetwarzania;

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

XI. POWOŁANIE INSPEKTORA OCHRONY DANYCH

Administrator danych powołuje inspektora ochrony danych. Jego powołanie/odwołanie zgłasza się Prezesowi Urzędu Ochrony Danych Osobowych w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora.

Do zadań inspektora ochrony danych należą:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów RODO oraz ustawy o ochronie danych osobowych;
- monitorowanie przestrzegania przepisów RODO oraz ustawy o ochronie danych osobowych oraz Polityki ochrony danych obowiązującej w jednostce, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
- współpraca z organem nadzorczym tj. Prezesem Urzędu Ochrony Danych Osobowych;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

XII. ZADANIA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

Administrator systemu informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych. W związku z tym:

- zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych i serwera z pozycji administratora,
- przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
- przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- przeprowadza szkolenie stanowiskowe użytkownika w zakresie korzystania ze sprzętu komputerowego i zasobów sieci, zapoznaje z obowiązującymi w tym zakresie dokumentami,
- nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
- w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje administratora danych/inspektora ochrony danych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
- prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
- sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
- podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

XIII. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

W przypadku zlecania przetwarzania danych osobowych podmiotom zewnętrznym administrator danych zobowiązany jest zawrzeć umowę powierzenia. W jednostce prowadzony jest rejestr umów powierzenia przetwarzania danych osobowych.

Umowa określa kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ponadto zobowiązuje podmiot przetwarzający do:

a) przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

b) zapewniania, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

c) podejmowania wszelkich środków wymaganych na mocy art. 32 RODO;

d) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego;

e) pomagania administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;

f) pomagania administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;

g) usuwania lub zwracania administratorowi danych osobowych oraz usuwania wszelkich istniejących kopii, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w przepisach RODO oraz umożliwiania administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

XIV. CZYNNOŚCI KONTROLNE

Nadzór i kontrolę nad ochroną danych osobowych sprawuje inspektor ochrony danych w porozumieniu z Dyrektorem Liceum i Administratorem systemów informatycznych.

Czynności kontrolne przeprowadzane są na bieżąco oraz raz w roku w formie pisemnego audytu. Z czynności kontrolnych sporządza się protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności, a także zalecenia i działania naprawcze. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne.

XV. REGULAMIN OCHRONY DANYCH OSOBOWYCH I SZKOLENIA WEWNĘTRZNE

Administrator danych wprowadza w Liceum Regulamin ochrony danych osobowych w celu zapewnienia osobom przetwarzającym dane osobowe pełny zakres wiedzy na temat zasad przetwarzania danych osobowych w jednostce oraz obciążających je obowiązków z tym związanych. Osoby zapoznane z Regulaminem zobowiązane są potwierdzić fakt zapoznania się z tym dokumentem oraz zdeklarować stosowanie się do jego zasad. Każda osoba przed zatrudnieniem powinna zostać zapoznana z Regulaminem. Administrator danych zapewnia również przeszkolenie pracowników z zakresu stosowania przepisów dotyczących ochrony danych osobowych, a obecność pracowników należy potwierdzić pisemnie.

XVI. AKTUALIZACJA POLITYKI OCHRONY DANYCH

W związku z dynamiką zmian w zakresie bezpieczeństwa informacji oraz dużym prawdopodobieństwem wprowadzania zmian w konstrukcji systemów informatycznych, Administrator danych zobowiązuje się dokonywać corocznie przeglądu i aktualizacji Polityki Bezpieczeństwa. Weryfikacja zapisów Polityki Ochrony Danych jest prowadzona pod kątem zgodności stanu deklarowanego ze stanem faktycznym.

Do końca każdego roku kalendarzowego Administrator Danych lub osoba przez niego upoważniona dokona sprawdzenia aktualności Polityki Ochrony Danych i przygotuje projekt ewentualnych zmian.

Polityka bezpieczeństwa podlega aktualizacji każdorazowo w przypadku likwidacji, utworzenia lub zmiany zawartości zbioru danych, a także w przypadku zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej jej aktualizacji.

Aktualizacja Polityki jest przeprowadzana przez Administratora Danych. Nowa wersja Ochrony Danych zastępuje poprzednio obowiązującą. Administrator Danych wprowadza w życie nową wersję Polityki Ochrony Danych w formie zarządzenia, określając w jego treści termin, od kiedy nowy dokument obowiązuje.

Administrator danych jest zobowiązany do poinformowania pracowników o zmianach i zapoznania z nową wersją przed dniem wejścia w życie.

Niezastosowanie się do prowadzonej przez administratora danych Polityki Ochrony Danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

XVII. NADAWANIE I REJESTROWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w Liceum.
2. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ASI.
3. ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez ADO.
4. Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.
5. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

XVIII. ZABEZPIECZENIE DANYCH W SYSTEMIE INFORMATYCZNYM

W Liceum wprowadza się tzw. Politykę haseł. Zgodnie z nią hasła powinny składać się przynajmniej z 8 znaków i zawierać duże litery + małe litery + cyfry (lub znaki specjalne). Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, ciągów liczbowych. Hasła nie mogą być ujawnianie innym osobom, zwłaszcza uczniom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.

W przypadku ujawnienia hasła – należy natychmiast je zmienić. Hasła muszą być zmieniane co 60 dni. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła. Hasła użytkowników uprzywilejowanych posiadających uprawnienia na poziomie administratorów systemów informatycznych objęte są takimi samymi restrykcjami dotyczącymi ich poufności jak pozostałe hasła.

System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

a. rozpoczęcie i zakończenie pracy przez użytkownika systemu,
b. operacje wykonywane na przetwarzanych danych,
c. nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
d. błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
2. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:
a. identyfikatora osoby, której dane dotyczą,
b. osoby przesyłającej dane,
c. odbiorcy danych,
d. zakresu przekazanych danych osobowych,
e. daty operacji
f. sposobu przekazania danych

3. Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania") na każdym komputerze, na którym przetwarzane są dane osobowe.
4. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

XIX. ZASADY BEZPIECZEŃSTWA PODCZAS PRACY W SYSTEMIE INFORMATYCZNYM

1. W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
a. loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła,
b. loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła
2. W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z sytemu lub uruchomienie wygaszacza ekranu chronionego hasłem.
3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.
5. Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone poinformowaniem pracowników Szkoły przez ASI na co najmniej 30 minut przed planowanym zawieszeniem.
6. Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ASI w razie:
a. podejrzenia naruszenia bezpieczeństwa systemu,
b. braku możliwości zalogowania się użytkownika na jego konto,
c. stwierdzenia fizycznej ingerencji w przetwarzana dane,
d. stwierdzenia użytkowania narzędzia programowego lub sprzętowego.
7. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:
a. nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem),
b. wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach),
c. różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych),
d. inne nadzwyczajne sytuacje.

XX. TWORZENIE KOPII ZAPASOWYCH

1. Dane systemów kopiowane są w trybie tygodniowym. Kopie awaryjne danych zapisywanych w programach wykonywane są co tydzień (w ostatni dzień roboczy tygodnia po zakończeniu pracy). Kopie programów i narzędzi programowych służących do przetwarzania danych tworzy się metodą całościową każdorazowo przed aktualizacją na macierzy dyskowej.
2. Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest ASI lub pracownik obsługujący dany program przetwarzający dane.
3. Dodatkowe kopie i kopie awaryjne przechowywane są w szafie pancernej w sekretariacie szkoły.
4. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ASI.
5. Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

XXI.UDOSTĘPNIENIE DANYCH

Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa.

XXII. PRZEGLĄDY I KONSERWACJE SYSTEMÓW

1. ASI dokonuje przeglądów i konserwacji systemów zgodnie z zaleceniami producenta oraz administratora ochrony danych, ale nie rzadziej niż co 3 miesiące. ASI powinien prowadzić dokumentację przeglądów i konserwacji, która powinna zawierać:

- czas i dat ę rozpoczęcia przeglądu/konserwacji,

- zakres wykonanych prac,

- wykaz osób zaangażowanych w przegląd/konserwację.

2. Prace wymienione w pkt. 1 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

XXIII. NISZCZENIE WYDRUKÓW I NOŚNIKÓW DANYCH

1. Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek.
2. Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć.
4. Po wykorzystaniu wydruki zawierające dane osobowe powinny być niszczone w niszczarce.

XXIII. PROCEDURA POSTĘPOWANIA Z INCYDENTAMI

Administrator danych wprowadza do stosowania procedurę postępowania z incydentami naruszenia ochrony danych osobowych. Celem tej procedury jest wypełnienie obowiązku wynikającego z art. 33 RODO. Procedura określa sposób definiowania incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie, a także procedurę wprowadzenia działań naprawczych. Każda osoba upoważniona do przetwarzania danych osobowych ma obowiązek poinformowania o możliwości wystąpienia incydentu lub o jego wystąpieniu. Taka informacja powinna być przekazana Inspektorowi ochrony danych bądź dyrektorowi Liceum.
Powiadomienia wymagają:

- niewłaściwe zabezpieczenie sprzętu elektronicznego, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych, udostępnienie haseł osobom postronnym,
- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, przyklejanie kartek z hasłami w szufladach),
- ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
- dokumentacja zawierająca dane osobowe niszczona bez użycia niszczarki,
- otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
- obecność osób postronnych w jednostce,
- złe ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
- wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz jednostki bez upoważnienia administratora danych,
- awarie serwera, komputerów, twardych dysków, oprogramowania,
- udostępnienie danych osobowych osobom nieupoważnionym,
- telefoniczne próby wyłudzenia danych osobowych,
- kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive z danymi osobowymi,
- maile nakłaniające do ujawnienia identyfikatora lub hasła,
- zainfekowanie komputerów wirusem lub inne błędne zachowanie komputerów,
- zdarzenia losowe (pożar obiektu, zalanie wodą, utrata zasilania, utrata łączności),
- włamanie do systemu informatycznego lub pomieszczeń,
- kradzież danych/sprzętu,
- świadome zniszczenie dokumentów.

Należy również powiadomić administratora systemów informatycznych. Ponadto należy udokumentować wystąpienie incydentu, jego skutki oraz podjęte działania naprawcze i zaradcze. W przypadku gdy incydent skutkuje naruszeniem praw lub wolności osób fizycznych, administrator danych zgłasza je w ciągu 72 godzin Prezesowi Urzędu Ochrony Danych Osobowych oraz gdy istnieje taki wymóg, powiadamia o tym fakcie osoby, których incydent dotyczył.