# DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH w I LICEUM OGÓLNOKSZTAŁCĄCYM IM. ADAMA ASNYKA w Kaliszu

**Administrator Danych Osobowych:**

**I Liceum Ogólnokształcące**

**im. Adama Asnyka**

**ul. Grodzka 1, 62-800 Kalisz**

**SPIS TREŚCI:**



## POLITYKA BEZPIECZEŃSTWA



## INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

# 1. WPROWADZENIE

Tworzy się dokumentację ochrony danych osobowych celem opisu sposobu przetwarzania danych osobowych oraz opisu środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Jednym z głównych celów dokumentacji jest przekazanie pracownikom I Liceum Ogólnokształcącego im. Adama Asnyka w Kaliszu podstawowej wiedzy z zakresu ochrony danych osobowych oraz zasad i procedur zwiększając świadomość pracowników o wartości posiadanych i przetwarzanych danych osobowych m.in. poprzez:

- wyjaśnienie zagadnienia i opisanie podstaw prawnych;
- scharakteryzowanie podstawowych zagrożeń bezpieczeństwa oraz sposób postępowania w przypadku ich wykrycia;
- opis zastosowanej polityki bezpieczeństwa;
- szczegółowy opis procedur pracy w systemach informatycznych;
- wykaz rejestru czynności ochrony danych osobowych;
- ocenę ryzyka w zakresie przetwarzania danych osobowych;
- zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi.

Stosując zasady zawarte w niniejszej dokumentacji, ryzyko wystąpienia negatywnych konsekwencji wynikających z zagrożeń przetwarzania danych osobowych takich jak:

- naruszenie interesów lub praw osoby fizycznej, której dane osobowe dotyczą;
- naruszenia danych osobowych rozumianych jako dobro prywatne powierzone I LO;
- naruszenie przepisów prawa;
- utraty lub obniżenia reputacji I LO mogącej mieć wpływ na jej wartość;
- strat finansowych ponoszonych w wyniku nałożonych kar lub utraty wiarygodności;
- zakłócenie czynności spowodowanych nieprawidłowym działaniem systemów informatycznych

jest zminimalizowane.

I Liceum Ogólnokształcące im. Adama Asnyka w Kaliszu realizuje zadania w zakresie edukacji, określone w ustawie z dnia 14 grudnia 2016 r. - Prawo oświatowe ze zmianami oraz z dnia 26 stycznia 1982 r. - Karta Nauczyciela ze zmianami.

# 2. PODSTAWA PRAWNA

Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

# 3. DEFINICJE

W dokumencie przyjmuje się następującą terminologię:

**I LO** – I Liceum Ogólnokształcące im. Adama Asnyka w Kaliszu

**RODO** - Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r.

**Ustawa** - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych ze zmianami.

**Dane osobowe** - 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.

**Przetwarzania** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

**Dane wrażliwe** - dane o pochodzeniu rasowym lub etnicznym, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa, partyjna lub związkowa, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

**Administrator danych (ADO)** – I Liceum Ogólnokształcące im. Adama Asnyka z siedzibą w Kaliszu, ul. Grodzka 1.

**Inspektor ochrony danych (IOD)** – osoba fizyczna wspierająca administratora danych w realizacji obowiązków dotyczących ochrony danych osobowych oraz nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną. Osoba powołana przez ADO.

**Administrator systemu informatycznego (ASI)** – osoba odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych przetwarzających dane osobowe. Osoba powołana przez ADO.

**Zbiór danych** - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

**System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

**Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

**Zgoda osoby, której dane dotyczą** – 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.

**Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

**Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

**Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

**Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

**Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

**Niezawodność** – właściwość zapewniająca, że zamierzone zachowania i skutki są spójne.

**Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

**Dokumentacja** – dokumentacja przetwarzania danych osobowych opisująca sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, określoną w przepisach prawnych.

# 4. WPROWADZENIE DO OCHRONY DANYCH OSOBOWYCH

Poniżej przedstawiono wyciąg najważniejszych informacji odnośnie ochrony danych osobowych.

## 4.1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

## 4.2. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

- swojej tożsamości i danych kontaktowych oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe inspektora ochrony danych;
- celu przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
- prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania takie jak: okres, przez który dane osobowe będą przechowywane, prawa osoby fizycznej, czy podanie danych jest konieczne j jakie są ewentualnie konsekwencje niepodania danych, informacje o zautomatyzowanym podejmowaniu decyzji.

Informacje powyższe przekazuje się również w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą, wraz z podaniem źródła pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.

Powyższych zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub osoba, której dane dotyczą, posiada już te informacje.

## 4.3. Przetwarzanie danych jest zabronione w przypadku:

- przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzanie powyższych danych, jest jednak dopuszczalne, jeżeli m.in.:

- osoba, której dane dotyczą, wyrazi na to zgodę na piśmie;
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą;

- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym;
- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy;
- przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

## 4.5. Zasady dotyczące przetwarzania danych osobowych:

Aby przetwarzać dane osobowe muszą one być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
- prawidłowe i w razie potrzeby uaktualniane;
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem;

Administrator danych jest odpowiedzialny za przestrzeganie powyższych zasad.

## 4.5. Prawa osoby, której dane dotyczą:

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do m.in.:

- dostępu do danych i ich poprawiania, przenoszenia danych;
- cofnięcia zgody na przetwarzanie danych;
- ograniczenia przetwarzania danych, sprzeciwu przetwarzania;
- usunięcia danych („prawo do bycia zapomnianym");
- niepodlegania zautomatyzowanemu podejmowaniu decyzji, profilowaniu;
- wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych.

## 4.6. Prezes Urzędu Ochrony Danych Osobowych

Organem nadzorczym do spraw ochrony danych osobowych w Polsce jest Urząd Ochrony Danych Osobowych (Prezes Urzędu Ochrony Danych Osobowych).

Do zadań Prezesa Urzędu Ochrony Danych Osobowych w szczególności należy m.in.:

- monitorowanie i egzekwowanie stosowania przepisów o ochronie danych osobowych;
- współpraca innymi organami nadzorczymi;
- wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych;
- inicjowanie i podejmowanie przedsięwzięć oraz doradzanie w zakresie upowszechniania i doskonalenia wiedzy z zakresu ochrony danych osobowych.

## 4.7. Obowiązki Administratora Danych Osobowych

Administrator Danych Osobowych (ADO) zobowiązany jest do zapewnienia zgodności przetwarzania danych osobowych z przepisami prawa, ochrony przetwarzania danych osobowych przed ich

udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, zbieraniem i przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Ponadto ADO zobowiązany jest zapewnić kontrolę i rozliczalność nad tym, jakie dane osobowe, kiedy i przez kogo są przetwarzane oraz komu są przekazywane.

W tym celu ADO prowadzi dokumentację oraz wszelkie potrzebne ewidencje i upoważnienia.

ADO, w przypadku podmiotów publicznych, obowiązany jest powołać Inspektora Ochrony Danych (IOD) oraz może powołać Administratora Systemu Informatycznego (ASI). Szczegółowe zadania IOD i ASI wykazane są w dalszej części dokumentacji.

# 5. ZAGROŻENIA BEZPIECZEŃSTWA

Charakterystyka możliwych zagrożeń:

**Zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona, lecz nie dochodzi do naruszenia poufności danych.

**Zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych.

**Zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

Poniżej przedstawiono przykładowe sytuacje świadczące o naruszeniu zasad bezpieczeństwa. W przypadku zaistnienia lub stwierdzenia podejrzenia wystąpienia któregokolwiek z zagrożeń należy niezwłocznie powiadomić ADO lub IOD:

**Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych** na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.

**Sytuacje przypadkowe** - pozostawienie niezamkniętych drzwi lub okien w pomieszczeniach gdzie przetwarza się dane osobowe w przypadku gdy w pomieszczeniu nie ma osób uprawnionych.

**Niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych.

**Awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu oraz sam fakt pozostawienia serwisantów bez nadzoru.

**Pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.

**Jakość danych w systemie** lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.

**Naruszenie** lub próba naruszenia integralności systemu lub bazy danych w tym systemie.

**Próba lub modyfikacja danych** oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (uwierzytelnienia).

**Niedopuszczalna manipulacja** danymi osobowymi w systemie.

**Ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu.

**Praca w systemie informatycznym wykazująca nieprzypadkowe odstępstwa** od założonego rytmu pracy oraz wskazująca na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.

**Podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony, kasowania lub kopiowanie danych.

**Rażące naruszenia dyscypliny pracy w systemie informatycznym w zakresie przestrzegania procedur bezpieczeństwa informacji** (niewylogowanie się przed opuszczeniem stanowiska pracy, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

**Zapisywanie danych osobowych na niezabezpieczonych nośnikach zewnętrznych** oraz wynoszenie ich poza obszar przetwarzania lub przesyłanie niezabezpieczonych danych przez internet.

**Rażące naruszenia dyscypliny przetwarzania danych papierowych w zakresie przestrzegania procedur bezpieczeństwa informacji** (pozostawienie danych na biurkach, półkach, pozostawienie otwartych szaf, przechowywanie dokumentów w miejscach do tego nieprzeznaczonych, wyrzucanie dokumentów z danymi osobowymi bez uprzedniego zniszczenia, pozostawienie danych osobowych w drukarce, na ksero, itp).

**Nieuprawnione instalowanie** jakiegokolwiek oprogramowania, obecność podejrzanego oprogramowania.

**Awarie sprzętu i oprogramowania**, w tym zasilaczy awaryjnych podtrzymujących zasilanie.

**Nieoczekiwane, niewyjaśnione i niezapowiedziane zmiany** w działaniu, wyglądzie oprogramowania, urządzenia, kabli.

**Nieuzasadnione przeglądanie danych** w ramach konsultacji lub pomocy technicznej.

**Pozostawienie nośników danych, wydruków, kserokopii, pism** i innych dokumentów zawierających dane osobowe w miejscach narażonych na łatwy dostęp osób trzecich.

**Nieuzgodnione, nieoczekiwane, nagłe wizyty** osób próbujących ingerować w system celem naprawy, konfiguracji lub kontroli.