# POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

## LICEUM OGÓLNOKSZTAŁCĄCE W TARNOWIE PODGÓRNYM

Tarnowo Podgórne, dnia

Podpis osoby zatwierdzającej

## Spis treści

## 1. Wprowadzenie

1.1. Polityka bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014r., poz. 1182 z późn. zmianami) oraz w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r, Nr 100, poz. 1024).

1.2. Polityka bezpieczeństwa obejmuje swoim zakresem zbiory danych osobowych, które przetwarzane są przez Liceum Ogólnokształcącym w Tarnowie Podgórnym (zwanym w dalszej części Polityki „Liceum").

1.3. Podstawy prawne i normatywne w zakresie Polityki bezpieczeństwa danych osobowych stanowią:

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182 z późn. zmianami),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100 poz. 1024);
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. wsprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r., Nr 229, poz. 1536),
- Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. 2002 r. Nr 23 poz. 225 z późn. zm.),
- Norma PN ISO 27001 dotycząca Systemu Zarządzania Bezpieczeństwem Informacji w Przedsiębiorstwach, w zakresie ochrony danych osobowych.

1.4. Zasady określone przez dokument Polityka bezpieczeństwa mają zastosowanie do:

- Danych osobowych przetwarzanych przez Liceum, zarówno w przypadku, gdy jest on administratorem danych, jak i w sytuacji, gdy przetwarza dane powierzone jemu na podstawie umów zawartych w trybie art. 31 Ustawy o ochronie danych osobowych;

- Wszystkich nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe podlegające ochronie;
- Wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe podlegające ochronie;
- Wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do danych osobowych podlegających ochronie.

1.5. Celemniniejszej Polityki bezpieczeństwa jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczać dane osobowe, a zatem organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych osobowych oraz edukowanie użytkowników systemu ochrony danych osobowych. Polityka bezpieczeństwa określa zadania związane z zachowaniem poufności, integralności oraz rozliczalności danych osobowych.

1.6. Polityka bezpieczeństwa dotyczy zadań związanych z zabezpieczeniem danych osobowych zarówno przetwarzanych w sposób papierowy i w systemach informatycznych. Osoby stanowiące personel Szkoły, a pracujące z danymi osobowymi zobowiązane są do przestrzegania postanowień Polityki.

1.7. Polityka bezpieczeństwa powinna być poddawana bieżącej aktualizacji, ale nie rzadziej niż raz do roku.

1.8. Jeżeli przepisy innych Ustaw przewidują dalej idącą ochronę danych osobowych niż Ustawa o ochronie danych osobowych, stosuje się przepisy tych Ustaw.

1.9. Naruszanie Ustawy o ochronie danych osobowych zagrożone jest następującymi konsekwencjami karnymi określonymi w jej zapisach:

- Art. 49 - za przetwarzanie danych osobowych bez podstawy prawnej - ograniczenie lub pozbawienie wolności do 2 lat,
- Art. 51 - za udostępnienie lub umożliwienie dostępu do danych osobom nieupoważnionym - ograniczenie lub pozbawienie wolności do 2 lat,
- Art. 52 - za niezabezpieczenie danych w odpowiedni sposób przed zabraniem, uszkodzeniem lub zniszczeniem przez osobę nieuprawnioną - ograniczenie lub pozbawienie wolności do roku,
- Art. 53 - za niezgłoszenie zbioru danych do rejestracji - ograniczenie lub pozbawienie wolności do 2 lat,
- Art. 54 - za niedopełnienie obowiązku poinformowania osoby, której dane dotyczą, o jej prawach, lub nieprzekazanie tej osobie informacji umożliwiających

korzystanie z praw przyznanych jej w niniejszej ustawie - ograniczenie lub pozbawienie wolności do 1 roku,

- Art. 54a - za udaremnianie lub utrudnianie wykonania czynności kontrolnej - ograniczenie lub pozbawienie wolności do 2 lat.

## 2. Podstawowe definicje

2.1. Administrator Danych Osobowych (zwany dalej ADO) – Liceum, decyduje o celach i środkach przetwarzania danych osobowych, jego przedstawicielem podejmującym wszelkie decyzje związane z bezpiecznym przetwarzaniem danych osobowych jest Dyrektor Liceum.

2.2. Administrator Bezpieczeństwa Informacji (ABI) – osoba wyznaczona przez ADO do nadzorowania przestrzegania zasad ochrony danych osobowych.

2.3. Administrator Systemu Informatycznego (ASI) - osoba wyznaczona przez ADO do nadzorowania i przestrzegania zasad ochrony danych osobowych w systemach informatycznych.

2.4. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzane przez administratora danych zarówno w systemach informatycznych jak i tradycyjnie w wersji papierowej.

2.5. GIODO - Generalny Inspektor Ochrony Danych Osobowych.

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

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

2.8. Nośniki danych – wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski, dyskietki, dyski CD-ROM, karty magnetyczne lub pamięci przenośne.

2.9. Odbiorca danych - każdy, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela podmiotu przetwarzającego dane osobowe mający siedzibę lub miejsce zamieszkania w państwie trzecim, podmiotu, któremu powierzono przetwarzanie danych osobowych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

2.10. Personel – osoby zatrudnione na podstawie stosunku pracy, umów cywilnoprawnych (umowa o dzieło, umowa zlecenia), przedsiębiorcy wykonujący

działalność osobiście i jednoosobowo, osoby odbywające praktyki, stażyści, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej wykonujące prace związane z przetwarzaniem danych osobowych u ADO.

2.11. Poufność danych - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom bądź podmiotom.

2.12. Przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, w szczególności w systemach informatycznych.

2.13. Rozliczalność – właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

2.14. System informatyczny – zespół urządzeń, sprzętu komputerowego, oprogramowania oraz baz danych przetwarzających dane osobowe.

2.15. Zbiór danych osobowych– każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

## 3. Administrator Danych Osobowych – obowiązki i odpowiedzialność

Do podstawowych obowiązków ADO należy:

3.1. Zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zabezpieczeniem danych przed:

- Udostępnieniem osobom nieupoważnionym,
- Zabraniem przez osobę nieuprawnioną,
- Zmianą, utratą, uszkodzeniem lub zniszczeniem.

3.2. Zapewnienie legalności przetwarzania danych osobowych, a w szczególności zadbanie, by:

- Została pozyskana zgoda osoby, której dane dotyczą lub została spełniona inna przesłanka dopuszczająca przetwarzanie danych osobowych,
- Został spełniony obowiązek informacyjny wobec osoby, której dane dotyczą,
- Dane były przetwarzane zgodnie z obowiązującymi przepisami prawa oraz normami i dobrymi praktykami oraz normami społecznymi,
- Dane zbierane były w oznaczonym zgodnym z prawem celem,

- Dane były merytorycznie poprawne oraz zakres danych był adekwatny do celu zbierania,
- Były przetwarzane z ograniczeniem czasowym.

3.3. Prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych, w szczególności:

- Polityki bezpieczeństwa danych osobowych,
- Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.

3.4. Wyznaczenie ABI nadzorującego przestrzeganie zasad ochrony w przypadku, w którym ADO nie wykonuje tych obowiązków sam.

3.5. Dopuszczanie do przetwarzania danych wyłącznie osoby przeszkolonej i posiadającej imienne upoważnienie, oraz wydawanie i zarządzanie upoważnieniami.

3.6. Nadzorowanie i dbanie o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).

3.7. Respektowanie prawa osób, których dane dotyczą, a w szczególności prawa do uzyskania informacji o:

- ADO,
- Celu, zakresie i sposobie przetwarzania danych,
- Terminu od kiedy i jakie dane są przetwarzane,
- Źródle, z którego dane pochodzą,
- Sposobie udostępniania danych oraz ich odbiorcach.

3.8. Respektowanie praw osób, których dane dotyczą w zakresie:

- Żądania uzupełnienia, uaktualnienia, sprostowania danych,
- Wniesienia umotywowanego wniosku do zaprzestania przetwarzania danych.

3.9. Wykonywanie rejestracji i aktualizacji zbiorów danych w rejestrze prowadzonym przez GIODO.

3.10. Przeprowadzanie regularnych wewnętrznych audytów przestrzegania przepisów dotyczących ochrony danych osobowych.

## 4. Administrator Bezpieczeństwa Informacji –obowiązki i odpowiedzialność

Obowiązki ABI obejmują:

4.1. Sporządzanie i wprowadzenie w życie zasad bezpiecznego przetwarzania danych osobowych, w szczególności w systemach informatycznych.

4.2. Opracowanie i aktualizację „Polityki bezpieczeństwa" zawierającej strategię ochrony danych przetwarzanych w systemach informatycznych oraz nadzorowanie przestrzegania określonych w niej zasad.

4.3. Opracowanie wraz z ASI „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych" i czuwanie nad jej przestrzeganiem.

4.4. Prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez Liceum.

4.5. Prowadzenie i aktualizacja ewidencji osób upoważnionych do przetwarzania danych osobowych.

4.6. Zarządzanie upoważnieniami do przetwarzania danych osobowych.

4.7. Nadzorowanie obiegu oraz przechowywania dokumentów zawierających dane osobowe.

4.8. Uczestniczenie w czynnościach kontrolnych GIODO.

4.9. Nadzorowanie fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe, w tym nadzorowanie dostępu do tych pomieszczeń oraz kontrolę przebywających w nich osób.

4.10. Nadzorowanie szkoleń personelu z zakresu bezpieczeństwa przetwarzania danych osobowych.

4.11. Nadzorowanie bieżących procesów przetwarzania danych, w tym analizę sytuacji oraz przyczyn, które doprowadziły do naruszenia zasad bezpieczeństwa.

4.12. Podczas realizacji swych zadań, ABI ma prawo do:

- Uzyskiwania wszelkich informacji dotyczących przetwarzanych danych osobowych od wszystkich komórek organizacyjnych,
- Kontrolowania komórek organizacyjnych pod kątem właściwego zabezpieczenia pomieszczeń oraz systemów informatycznych, w których przetwarzane są dane osobowe,
- Proponowania ADO rozwiązań dotyczących ochrony danych osobowych,
- Wydawania orzeczeń dotyczących właściwego zbierania i przekazywania danych osobowych,
- Żądania od personelu udzielenia wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych lub w związku z nieprawidłowościami lub zagrożeniami związanymi z ochroną danych osobowych.

## 5. Administrator Systemu Informatycznego – zadania i odpowiedzialność

Obowiązki ASI obejmują:

5.1. Przestrzeganie zasad ochrony danych osobowych określonych w „Polityce bezpieczeństwa" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" i dokumentach z nimi związanych.

5.2. Zapewnienie prawidłowej eksploatacji systemu informatycznego, zgodnej z celami przetwarzania danych osobowych.

5.3. Nadzorowanie wykonywania kopii zapasowych, odpowiedniego ich przechowywania oraz okresowego sprawdzania pod kątem ich dalszej przydatności do odtwarzania danych osobowych w przypadku awarii systemu.

5.4. Zapewnienie ochrony nośników zawierających kopie zbiorów danych osobowych.

5.5. Realizację wytycznych ABI w zakresie ochrony danych osobowych przetwarzanych z wykorzystaniem środków informatycznych.

5.6. Informowanie ABI i ADO o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych przetwarzanych w systemach informatycznych.

5.7. Wyjaśnianie – wspólnie z ABI – wszystkich zgłoszonych nieprawidłowości i incydentów.

## 6. Pracownicy Liceum

6.1. Wszyscy pracownicy Liceum posiadający upoważnienie do przetwarzania danych osobowych zobowiązani są do zapoznania się z treścią dokumentacji określającą sposób postępowania przy ich przetwarzaniu.

6.2. Każdy pracownik podpisuje oświadczenie zawierające deklarację znajomości i stosowania wymogów określonej w pkt. 6.1. dokumentacji (Załącznik nr 2 Polityki).

6.3. Oświadczenia, o których mowa powyżej przechowywane są w aktach osobowych pracownika.

## 7. Obowiązek informacyjny

7.1. W przypadku zbierania danych osobowych na formularzach, umowach, drukach (zarówno papierowych jak i elektronicznych) należy umieszczać na nich odpowiednią klauzulę informacyjną. Klauzula taka powinna informować osobę, której dane zbieramy o:

7.1.1. Adresie siedziby i pełnej nazwie ADO.

7.1.2. Celu zbierania danych.

7.1.3. Prawie dostępu do treści swoich danych oraz ich poprawiania.

7.1.4. Dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

7.2. Przepisu określonego w ust. 1 nie stosuje się, jeżeli:

7.2.1. Przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania.

7.2.2. Osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1

7.3. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, ADO jest zobowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

7.3.1. Adresie siedziby i pełnej nazwie ADO.

7.3.2. Celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych.

7.3.3. Źródle danych.

7.3.4. Prawie dostępu do treści swoich danych oraz ich poprawiania.

7.3.5. Uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 Ustawy.

7.4. Przepisu określonego w ust. 1 nie stosuje się w przypadkach określonych w art. 25 ust. 2 pkt 1, 3 i 5 Ustawy.

## 8. Powierzanie przetwarzania danych osobowych

8.1. ADO może powierzyć przetwarzanie danych osobowych innemu podmiotowi na podstawie umowy powierzenia zawartej na piśmie.

8.2. Przekazanie zbiorów podmiotowi zewnętrznemu w celu ich przetwarzania nie powoduje zmiany właściwego ADO, którym pozostaje Liceum.

8.3. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych zobowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie.

8.4. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych obowiązany jest w szczególności do:

- Stosowania odpowiednich środków ochrony danych osobowych, w tym do zapewnienia fizycznej ochrony pomieszczeń w których przetwarzane są dane oraz tworzenia kopii bezpieczeństwa systemów informatycznych, w których przetwarzane są powierzone dane osobowe,

- Opracowania dokumentacji dotyczącej przetwarzania danych osobowych,
- Niezwłocznego powiadomienia Liceum o przypadkach naruszenia przetwarzania powierzonych danych osobowych oraz do dokumentowania wszelkich informacji, które mogą pomóc w ustaleniu okoliczności tego naruszenia,
- Zapewnienia, aby każda osoba stanowiąca personel podmiotu zewnętrznego przetwarzająca powierzone dane osobowe posiadała upoważnienie do przetwarzania tych danych osobowych,
- Zniszczenia lub zwrotu przekazanych danych stosownie do zapisów umowy powierzenia przetwarzania danych.

8.5. Wzór umowy powierzenia danych osobowych do przetwarzania podmiotowi zewnętrznemu stanowi Załącznik nr 5 Polityki.

8.6. Spis podmiotów przetwarzających dane osobowe na podstawie umowy powierzenia zawarty został w Załączniku nr 6 Polityki.

## 9. Zasady udostępniania danych osobowych

9.1. Udostępnianie danych jest jedną z form ich przetwarzania.

9.2. Udostępnianie danych osobowych odbiorcom danych może nastąpić, podobnie jak przetwarzanie danych, w przypadku spełnienia jednej z przesłanek określonych w art. 23 ust. 1 pkt 1-5 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, tj:

- Osoba, której dane dotyczą, wyrazi na to zgodę,
- Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- Jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- Jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

9.3. Osoby upoważnione do przetwarzania danych, którzy w ramach swych obowiązków służbowych udostępniają dane osobowe mają obowiązek prowadzić ewidencję danych, które są udostępniane (określającą odbiorcę danych, przyczynę udostępnienia, zakres danych oraz datę udostępnienia).

9.4. Wzór ewidencji określonej w p. 8.3 stanowi Załącznik nr 7 Polityki.

## 10. Zbiory danych osobowych przetwarzane przez Liceum

Kompletna lista zbiorów danych osobowych przetwarzanych przez Szkołę została zawarta w Załączniku nr 1 Polityki.

## 11. Środki ochrony fizycznej

11.1. Wszystkie pomieszczenia Liceum, w których przetwarzane są dane osobowe zabezpieczone są od zewnątrz drzwiami zwykłymi bądź wzmacnianymi zamykanymi na klucz.

11.2. Obszar przetwarzania danych osobowych w Liceum podczas nieobecności pracowników został zabezpieczony sygnalizacją przeciwwłamaniową oraz pozostaje pod całodobowym monitoringiem ze strony firmy ochroniarskiej.

11.3. Osoby nieupoważnione mogą przebywać w pomieszczeniach wyłącznie w obecności osób upoważnionych z ramienia ADO i tylko w czasie wymaganym na wykonanie niezbędnych czynności

11.4. Dokumenty papierowe zawierające dane osobowe przechowywane są w szafach metalowych oraz niemetalowych zamykanych na klucz. Dostęp do kluczy do wskazanych miejsc mają tylko osoby upoważnione.

11.5. Po ustaniu przydatności dokumentacja papierowa zawierająca dane osobowe jest niszczona mechanicznie z użyciem niszczarki dokumentów.

11.6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, należy pozbawić wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.

11.7. Fizyczny dostęp do danych osobowych mają tylko osoby posiadające pisemne, imienne upoważnienia podpisane przez ADO lub osobę przez niego upoważnioną.

## 12. Środki sprzętowe, informatyczne i telekomunikacyjne

12.1. Dane osobowe przetwarzane przy użyciu systemu informatycznego są zabezpieczone przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla oraz programu antywirusowego.

12.2. Oprogramowanie antywirusowe oraz firewall wykrywa i eliminuje wirusy, konie trojańskie, robaki komputerowe oprogramowanie szpiegujące i kradnące hasła oraz inne niebezpieczne oprogramowanie.

12.3. Wszelkie systemy informatyczne ADO służące do przetwarzania danych osobowych mogą być wykorzystane wyłącznie w celach służbowych.

12.4. Zasoby systemu informatycznego przetwarzane mogą być wyłącznie zgodnie z ich przeznaczeniem.

12.5. Dostęp do systemu operacyjnego komputera oraz aplikacji, w których są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem indywidualnego identyfikatora użytkownika oraz hasła.

12.6. W związku z zastosowaniem przez ADO środków bezpieczeństwa na poziomie wysokim (określonych w p. 1 Załącznika do Rozporządzenia), hasło zabezpieczające musi się składać z minimum 8 znaków, zawierających małe i wielkie litery, cyfry lub znaki specjalne.

12.7. W związku z zastosowaniem środków bezpieczeństwa na poziomie wysokim hasło musi być zmieniane cyklicznie, nie rzadziej niż raz na 30 dni.

Szczegółowe wytyczne dotyczące polityki zarządzania hasłami, sposobie nadawania uprawnień do pracy w systemie informatycznym oraz zabezpieczeń sprzętowych i systemowych zostały określone w dokumencie „Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe dla Liceum Ogólnokształcącego w Tarnowie Podgórnym”.

## 13. Środki organizacyjne

13.1. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem ich do pracy z tymi danymi muszą zostaćprzeszkolone w zakresie obwiązujących przepisów o ochroniedanych osobowych, procedur przetwarzania danych oraz informowane o podstawowychzagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.

13.2. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych w Liceumwedług wzoru określonego w załączniku Nr 4.

13.3. Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działańkonserwacyjnych w systemie oraz naprawy systemu (Załącznik nr 2 Instrukcji).

13.4. Określono sposób postępowania z nośnikami informacji.

Załącznik nr 1

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez Liceum Ogólnokształcące w Tarnowie Podgórnym

**REJESTR ZBIORÓW DANYCH OSOBOWYCH**

1. Rodzaje i nazwy zbiorów danych osobowych.
   1.1. Zbiór danych osobowych kadrowo – płacowych pracowników zatrudnionych w Liceum.
   1.2. Zbiór danych osobowych kandydatów do pracy w Liceum.
   1.3. Zbiór danych osobowych książka korespondencji.
   1.4. Zbiór danych osobowych zawartych w umowach cywilno-prawnych.
   1.5. Zbiór danych osobowych uczniów Liceum oraz ich rodziców/opiekunów prawnych.(Księga ewidencji uczniów Liceum Ogólnokształcącego w Tarnowie Podgórnym)
   1.6. Zbiór danych osobowych kandydatów doLiceum.
2. Zakres danych osobowych przetwarzanych w zbiorach określonych w p. 1.
   2.1. W zbiorach dotyczących danych osobowych pracowników Liceum oraz kandydatów do pracy w Liceum:

- Nazwisko i imiona,
- Imiona rodziców,
- Data i miejsce urodzenia,
- Numer PESEL,
- Seria i numer dowodu osobistego
- Nazwisko rodowe,
- Obywatelstwo,
- Oddział NFZ
- Urząd skarbowy,
- Adres stałego zameldowania,
- Adres zamieszkania,
- Adres korespondencyjny,

- Wykształcenie,
- Staż pracy,
- Ilość godzin,
- Wynagrodzenie,
- Stosunek do służby wojskowej,
- Nr telefonu,
- Adres poczty email.

2.2. W zbiorach dotyczących danych osobowych dzieci – uczniów Liceum - i ich rodziców/opiekunów prawnych:

- Imiona i nazwisko,
- Data i miejsce urodzenia,
- Adres zamieszkania,
- PESEL,
- Imiona i nazwiska rodziców/opiekunów prawnych
- Numer telefonu oraz adres poczty email rodziców/opiekunów prawnych.

2.3. W zbiorze danych osobowych książka korespondencji przychodzącej i wychodzącej:

- Imię/imiona i nazwisko,
- Adres korespondencyjny (zamieszkania bądź inny).

3. Oprogramowanie i systemy komputerowe zastosowane do przetwarzania danych osobowych Liceum:

3.1. MS Windows.
3.2. MS Office.
3.3. Vulcan.
3.4. System Informacji Oświatowej (SIO).
3.5. Librus – dziennik elektroniczny. (e-Świadectwa)
3.6. Nabór (szkoły ponadgimnazjalne) Poznańskie Centrum Superkomputerowo-Sieciowe.
3.7. Hermes (aplikacja dla szkół ponadgimnazjalnych-egzaminy maturalne).
3.8. Mol (arkusz Optivum dla bibliotek).
3.9. Pielęgniarka (system zarządzania obiegiem informacji SZOI- NFZ)

4. Obszar przetwarzania danych osobowych:
   4.1. Pomieszczenia biurowo-administracyjne Liceum zlokalizowanew budynku przy ulicy Poznańskiej 118 w Tarnowie Podgórnym.
   4.2. Pomieszczenia w których odbywa się nauczanie uczniów zlokalizowane w budynku przy ulicy Poznańskiej 118 w Tarnowie Podgórnym.
   4.3. Pomieszczenie Pokoju Nauczycielskiego zlokalizowane w budynku Liceumprzy ulicy Poznańskiej 118 w Tarnowie Podgórnym.
   4.4. Pomieszczenie składnica akt Liceum zlokalizowane w budynku przy ulicy Poznańskiej 118 w Tarnowie Podgórnym.
   4.5. Pomieszczenie serwerownia(sala komputerowa) zlokalizowane w budynku Liceum przy ulicy Poznańskiej 118 w Tarnowie Podgórnym.
   4.6. Gabinet psychologa Liceum zlokalizowany w budynku przy ulicy Poznańskiej 118 w Tarnowie Podgórnym.
   4.7. Gabinet pielęgniarski Liceum zlokalizowany w budynku przy ulicy Poznańskiej 118 w Tarnowie Podgórnym.
   4.8. Pomieszczenie biblioteka Liceum zlokalizowane w budynku przy ulicy Poznańskiej 118 w Tarnowie Podgórnym.

Załącznik nr 2
(wzór)

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez Liceum Ogólnokształcące w Tarnowie Podgórnym

.....
(nazwisko i imię)
.....
(stanowisko)

**OŚWIADCZENIE**

Ja, niżej podpisany oświadczam, że przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/ny z przepisami dotyczącymi ochrony danych osobowych, a także z następującą dokumentacją:

1. Dokumentem „Polityka bezpieczeństwadanych osobowych w Liceum Ogólnokształcącym w Tarnowie Podgórnym”.
2. Dokumentem „Instrukcja zarzadzania systemem informatycznymw Liceum Ogólnokształcącym w Tarnowie Podgórnym”.

.....
(podpis oświadczającego)

Załącznik nr 3
(wzór)

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez Liceum Ogólnokształcące w Tarnowie Podgórnym

Tarnowo Podgórne, dnia ……

**UPOWAŻNIENIE**

Na podstawie Art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014, poz. 1182 z późn. zm.)

Upoważniam Panią/Pana…….. pracownika Liceum Ogólnokształcącego w Tarnowie Podgórnym do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie:

……..

ze szczególnym uwzględnieniem zadań zawartych w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Upoważnienie niniejsze nie upoważnia do udzielania dalszych upoważnień i wygasa z dniem ustania stosunku pracy, a ponadto może być w każdym czasie zmienione lub odwołane.

.....
(podpis w imieniu Administratora Danych Osobowych)

Załącznik nr 4

(wzór)

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez Liceum Ogólnokształcące w Tarnowie Podgórnym

**EWIDENCJA OSÓBUPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH**

| Nazwisko i imię | Stanowisko służbowe | Zakres upoważnienia do przetwarzania danych osobowych | Nr upoważnienia | Data nadania upoważnienia | Data ustania upoważnienia | Identyfikator ( jeśli dane przetwarzane są w systemie informatycznym) |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

Załącznik nr 5

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez Liceum Ogólnokształcące w Tarnowie Podgórnym

**Umowa powierzenia czynności przetwarzania danych osobowych**

Zawarta w dniu ..... w …….

Pomiędzy

……

reprezentowanym przez:

……. - ……

zwanymi w dalszej części Umowy**Powierzającym**a:

.....

zwaną w dalszej części Umowy **Przetwarzającym**

§ 1

Przedmiot umowy

1. W ramach umowy Powierzający, jako Administrator Danych Osobowych, na podstawie art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014, poz. 1182 z późn. zm.) powierza Przetwarzającemu przetwarzanie danych osobowych w związku z wykonywaniem czynności określonych w § 2 ust. 1 Umowy.

§2

Cel powierzenia

1. Powierzenie przetwarzania danych następuje w związku z następującymi czynnościami:
   1.1. Wszelkimi pracami związanymi z realizacją przedmiotu umowy zawartej pomiędzy Powierzającym a Przetwarzającym z dnia ……., nr umowy ……..
2. Przetwarzający zobowiązuje się przetwarzać powierzone dane osobowe jedynie w celu realizacji czynności określonych w § 2 niniejszej umowy.

§3

OświadczeniaPrzetwarzającego

1. Przetwarzający oświadcza, iż dysponuje odpowiednimi środkami, w tym należytymi zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z

2014, poz. 1182 z późn. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

2. Przetwarzający oświadcza, iż przygotował stosowną dokumentację wymaganą od podmiotu, któremu powierzono przetwarzanie danych osobowych, zgodnie z postanowieniami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014, poz. 1182 z późn. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

§4

## Odpowiedzialność Przetwarzającego

1. Zgodnie z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014, poz. 1182 z późn. zm.) Przetwarzający jest odpowiedzialny za ochronę powierzonych do przetwarzania danych osobowych na zasadach określonych w tej ustawie przewidzianych dla podmiotu, któremu powierzono przetwarzanie danych osobowych.

§5

## Środki zabezpieczające

1. W zakresie przestrzegania przepisów prawa dotyczących ochrony danych osobowych Przetwarzający ponosi odpowiedzialność taką samą jak administrator danych osobowych (Powierzający).

§6

## Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszą umową zastosowanie znajdują przepisy ustawy o ochronie danych osobowych, rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz innych przepisów.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

| | |
|---|---|
| …… | …… |
| Powierzający | Przetwarzający |

Załącznik nr 6

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez Liceum Ogólnokształcące w Tarnowie Podgórnym

**REJESTR PODMIOTÓW PRZETWARZAJĄCYCH DANE OSOBOWE NA PODSTAWIE UMOWY POWIERZENIA**

| LP | Nazwa Podmiotu | Zakres świadczonych usług | Nr umowy | Uwagi |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Załącznik nr 7

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez Liceum Ogólnokształcące w Tarnowie Podgórnym

**EWIDENCJA UDOSTĘPNIANIA DANYCH OSOBOWYCH**

| LP | Odbiorca danych osobowych (nazwa) | Przyczyna udostępnienia danych osobowych | Zakres udostępnionych danych | Data udostępnienia |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |