

Załącznik Nr 1 do Zarządzenia nr 1/18
Dyrektora Katolickiego Liceum
Ogólnokształcącego im. C. K. Norwida

Polityka ochrony danych osobowych

**przetwarzanych
w Katolickim Liceum Ogólnokształcącym
im. C. K. Norwida**

SPIS TREŚCI

- I.** Wstęp
- II.** Podstawowe pojęcia
- III.** Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych.
- IV.** Realizacja praw osób, których dane są przetwarzane w Szkole
- V.** Powierzenie przetwarzania danych osobowych
- VI.** Udostępnianie danych osobowych
- VII.** Analiza ryzyka
- VIII.** Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych
- IX.** Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej
- X.** Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych
- XI.** Naruszenie bezpieczeństwa danych osobowych
- XII.** Weryfikacja systemu ochrony danych
- XIII.** Postanowienia końcowe
- XIV.** Wykaz załączników

Załączniki 1 – 6

I. Wstęp

1. W dążeniu do zapewnienia wysokiego poziomu ochrony przetwarzanych danych osobowych, w tym zabezpieczenia danych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w Katolickim Liceum Ogólnokształcącym im. C. K. Norwida, określa się „Politykę ochrony danych osobowych przetwarzanych w Katolickim Liceum Ogólnokształcącym im. C. K. Norwida”.
2. Dyrektor Katolickiego Liceum Ogólnokształcącego im. C. K. Norwida, jako Administrator, zobowiązany jest do zabezpieczenia przetwarzanych danych osobowych, poprzez podjęcie środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia praw lub wolności osób fizycznych, z uwzględnieniem wiedzy technicznej, kosztów wdrożenia oraz charakteru, zakresu, kontekstu i celów przetwarzania.
3. Przetwarzanie danych osobowych, może być realizowane po spełnieniu jednego z warunków określonych w art. 6 RODO.
4. Niniejsza polityka ochrony obejmuje wszystkie procesy i czynności przetwarzania danych osobowych w Szkole i odnosi się do zabezpieczenia danych osobowych przetwarzanych zarówno w formie papierowej jak i przy wykorzystaniu systemów teleinformatycznych.

II. Podstawowe pojęcia

Ilekróć w niniejszym dokumencie jest mowa o:

- 1) Szkole – rozumie się przez to Katolickie Liceum Ogólnokształcące im. C. K. Norwida;
- 2) Administratorze – rozumie się przez to Dyrektora Szkoły;
- 3) RODO – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE L 119, s. 1);
- 4) Polityce – rozumie się przez to „Politykę ochrony danych osobowych przetwarzanych w Katolickim Liceum Ogólnokształcącym im. C. K. Norwida”;
- 5) IOD w przepisach rozporządzenia – rozumie się przez to inspektora ochrony danych osobowych. Powołanie inspektora nie obowiązuje w szkole prowadzonej przez podmiot niepubliczny – niebędący jednostką sektora finansów publicznych (zob. art. 37 RODO i art. 9 ODO).
- 6) ASI – rozumie się przez to administratora systemu informatycznego, czyli pracownika wyznaczonego przez Administratora, odpowiedzialnego za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie;
- 7) danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
- 8) przetwarzaniu danych osobowych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie,

organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

III. Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

1. Za bezpieczeństwo danych osobowych przetwarzanych w Szkole odpowiada Administrator, który w myśl przepisów RODO, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
2. Do zadań Administratora należy:
 - 1) wydawanie upoważnień do przetwarzania danych osobowych – wzór upoważnienia określa **załącznik nr 1**;
 - 2) odwoływanie upoważnień do przetwarzania danych osobowych – wzór odwołania upoważnienia określa **załącznik nr 2**;
 - 3) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych – wzór ewidencji określa **załącznik nr 3**,
 - 4) ewidencjonowanie oświadczeń osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa **załącznik nr 4**,
 - 5) określanie potrzeb w zakresie stosowanych w Szkole zabezpieczeń, zatwierdzanie rozwiązań i nadzorowanie prawidłowości ich wdrożenia,
 - 6) podnoszenie świadomości i kwalifikacji osób przetwarzających dane osobowe w Szkole i zapewnienie odpowiedniego poziomu przeszkolenia w tym zakresie,
Dyrektor – Administrator, może wyznaczyć pracownika administracyjnego, który będzie dbał o dokumentację i będzie podlegał dyrektorowi.
3. Do zadań ASI należy:
 - 1) zarządzanie bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami Administratora,
 - 2) doskonalenie metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
 - 3) przydzielanie identyfikatorów użytkownikom systemu informatycznego oraz zaznajamianie ich z procedurami ustalania i zmiany haseł dostępu,
 - 4) nadzorowanie prac związanych z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
 - 5) zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
 - 6) prowadzenie nadzoru nad archiwizacją zbiorów danych oraz zabezpieczanie elektronicznych nośników informacji zawierających dane osobowe.
4. Pracownik upoważniony do przetwarzania danych osobowych:
 - 1) chroni prawo do prywatności osób fizycznych powierzających Szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce;

- 2) zapoznaje się zasadami określonymi w Polityce i składa oświadczenie o znajomości tych przepisów;
- 3) za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą ponosi odpowiedzialność karną, wynikająca z przepisów ustawy o ochronie danych osobowych lub pracowniczą na zasadach określonych w kodeksie pracy.

IV. Realizacja praw osób, których dane są przetwarzane w Szkole

- I. W Szkole wprowadza się rozwiązania, które pozwalają na realizowanie praw osób, których dane są przetwarzane. W szczególności dotyczy to:
 - 1) umożliwienia osobom, których dane dotyczą wyrażenia zgody na przetwarzanie danych osobowych (gdy brak innej podstawy do przetwarzania danych),
 - 2) informowania osób, których dane dotyczą o zbieraniu i przetwarzaniu tych danych,
 - 3) prawa dostępu przysługującego osobom, których dane dotyczą,
 - 4) prawa osób, których dane dotyczą, do sprostowania danych,
 - 5) prawa osób, których dane dotyczą, do usunięcia swoich danych („prawa do bycia zapomnianym”),
 - 6) prawa osób, których dane dotyczą, do ograniczenia przetwarzania danych.
- II. Spełnienie obowiązków informacyjnych względem osób, których dane są przetwarzane odbywa się poprzez przekazanie osobom wymaganych prawem informacji przy zbieraniu danych oraz udokumentowanie realizacji tych obowiązków.
- III. Warunkiem prawidłowego spełnienia obowiązku informacyjnego wobec osoby, której dane dotyczą, jest przekazanie jej w zwięzłej, przejrzystej i zrozumiałej formie, jasnym i prostym językiem wszelkich informacji, o których mowa w art. 13 i 14 RODO oraz prowadzenie z nią wszelkiej korespondencji, w myśl art. 15-22 i 34 RODO w sprawie przetwarzania danych osobowych.
- IV. Informacji, o których mowa w pkt. 3 udziela się na piśmie, w tym w stosownych przypadkach – elektronicznie lub w inny sposób (np. ustnie).
- V. Informacje podawane na mocy art. 13 i 14 RODO oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 RODO są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nadmierne, w szczególności ze względu na swój ustawiczny charakter, Szkoła może pobrać opłatę uwzględniającą administracyjne koszty udzielenia informacji.
- VI. Realizacja zadań, o których mowa w pkt. 1 uwzględnia zasady, w tym wyłączenia, które zostały określone w obowiązujących przepisach prawa o ochronie danych osobowych.
- VII. Dostęp, usunięcie lub ograniczenie przetwarzania danych osobowych musi być zgodne z przepisami prawa, na podstawie których odbywa się przetwarzanie oraz na podstawie przepisów prawa określających zasady przetwarzania dokumentacji archiwalnej.

V. Powierzenie przetwarzania danych osobowych

1. Przetwarzanie powierzonych danych może być realizowane wyłącznie przez podmioty, które gwarantują odpowiednie środki techniczne i organizacyjne dające możliwość spełnienia wymogów RODO, w tym w szczególności skutecznie chroniło prawa osób, których dane dotyczą.
2. Przy określaniu minimalnych wymogów, które powinien spełnić podmiot przetwarzający należy brać pod uwagę charakter, skalę i zakres przetwarzania oraz, jeśli to konieczne, uwzględniać wyniki szacowania ryzyka przeprowadzone w Szkole w tym zakresie.
3. Powierzenie przetwarzania danych osobowych odbywa się na podstawie pisemnej umowy lub porozumienia, które wyraźnie określają charakter i cel przetwarzania, przedmiot i czas trwania przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, oraz obowiązki i prawa administratora i podmiotu przetwarzającego.
4. Dokumentacja, na podstawie której następuje powierzenie danych, musi mieć formę pisemną (dopuszcza się prowadzenie tej dokumentacji w formie elektronicznej).
5. Dokumentacja, na podstawie której następuje powierzenie danych, musi gwarantować Administratorowi realizację zadań wynikających z zapisów art. 28 RODO, w tym w szczególności:
 - 1) możliwość egzekwowania wskazanych w dokumentacji obowiązków podmiotu przetwarzającego,
 - 2) możliwość przeprowadzanie kontroli/audytów w zakresie realizacji umowy powierzenia,
 - 3) możliwości weryfikacji czy powierzone dane nie zostały przekazane innemu podmiotowi przez przetwarzającego bez zgody („podpowierzenie danych”).

VI. Udostępnianie danych osobowych

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia Administratora danych osobowych może mieć miejsce wyłącznie w przypadku działań osób i podmiotów uprawnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
2. Dane osobowe mogą być udostępniane:
 - 1) podmiotom i organom publicznym działającym w granicach przyznanych im uprawnień, po okazaniu dokumentów potwierdzających te uprawnienia;
 - 2) stronom postępowań administracyjnych prowadzonych w Szkole, na zasadach określonych w kodeksie postępowania administracyjnego lub odrębnych przepisów.
3. Administrator odmawia udostępnienia danych osobowych jeżeli spowodowałoby to naruszenie przepisów prawa.

VII. Analiza ryzyka

1. W trakcie procesu zarządzania ryzykiem przeprowadzana jest identyfikacja zagrożeń bezpieczeństwa danych osobowych oraz określane są podatności i skutki wystąpienia tych

zagrożeń oraz kategoryzacja danych i czynności przetwarzania pod kątem ryzyka, które przedstawiają.

2. W ramach procesu zarządzania ryzykiem przeprowadzana jest:
 - 1) analiza ryzyka dla czynności przetwarzania danych lub ich kategorii;
 - 2) ocena skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie.
3. Uzyskane, w ramach procesu analizy ryzyka, wyniki są podstawą do dalszego postępowania ze zidentyfikowanymi ryzykami w kontekście wdrożenia rozwiązań technicznych i organizacyjnych, które pozwolą ochronić dane osobowe przed utratą ich podstawowych atrybutów (poufności, integralności, dostępności, rozliczalności) oraz pozwolą zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania tych danych w Szkole.
4. Ocena skutków czynności przetwarzania dla ochrony danych oraz ich wpływu na naruszenia praw lub wolności osób fizycznych obejmuje analizę i rozpatrywanie możliwych sytuacji i scenariuszy naruszenia ochrony danych osobowych przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania, oraz różnego prawdopodobieństwa wystąpienia i wagi zagrożenia.
5. W ramach przeprowadzanej oceny, o której mowa w pkt. 4, należy brać pod uwagę wskazane przez Prezesa UODO rodzaje procesów i czynności przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych.

VIII. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

Szkoła nie przekazuje danych osobowych do państw trzecich lub organizacji międzynarodowych.

IX. Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

1. Pomieszczenia, w których przetwarzane są dane osobowe, pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia musi być poprzedzone przeniesieniem danych osobowych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.
2. Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych, w zakresie zgodnym z kategorią danych.
3. Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z Administratorem, w przypadku pracowników upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

X. Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w Instrukcji zarządzania systemem informatycznym, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego Szkoły, stanowiącej **załącznik nr 5**.

XI. Naruszenie bezpieczeństwa danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych w Szkole jest zobowiązana do natychmiastowego powiadamiania Administratora o wystąpieniu incydentu związanego z naruszeniem ochrony danych osobowych.
2. Szczegółowy tryb postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych, został określony w **załączniku nr 6**.

XII. Weryfikacja systemu ochrony danych

1. Weryfikacja systemu ochrony danych odbywa się poprzez prowadzenie kontroli okresowych nie rzadziej niż raz w roku.
2. W zależności od potrzeb, część prac w ramach weryfikacji systemu ochrony danych, może zostać zlecone podmiotowi zewnętrznemu.

XIII. Postanowienia końcowe

1. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszym dokumencie oraz pozostałej dokumentacji, która uszczegóławia wymagania i zasady ochrony danych osobowych.
2. Przypadki, niezasadzonego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako naruszenie obowiązków służbowych.
3. Polityka oraz pozostała dokumentacja, która uszczegóławia wymagania i zasady ochrony danych osobowych może być udostępniana osobom trzecim, jeżeli nie zawiera w swojej treści i w załącznikach szczegółowych informacji o wdrożonych w Szkole zabezpieczeniach danych osobowych oraz innych informacji prawnie chronionych.

XIV. Wykaz załączników

- Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych
- Załącznik nr 2 – Odwołanie upoważnienia
- Załącznik nr 3 – Ewidencja osób upoważnionych do przetwarzania danych osobowych
- Załącznik nr 4 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych
- Załącznik nr 5 – Instrukcja zarządzania systemem informatycznym

Załącznik nr 6 – Zasady postępowania w przypadku wykrycia naruszenia ochrony danych osobowych przetwarzanych w Katolickim Liceum Ogólnokształcącym im. C. K. Norwida

Garwolin, dnia r.

.....
(pieczęć Szkoły)

UPOWAŻNIENIE nr/20..... do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE L 119, s. 1)

upoważniam Panią/Pana
zatrudnioną(ego) w Katolickim Liceum Ogólnokształcącym im. C. K. Norwida do przetwarzania danych osobowych zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w zakresie wynikającym z zajmowanego stanowiska pracy, w okresie od dnia 20.... r. do odwołania upoważnienia.

Informuję, że Pani/Pan została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Szkole.

.....
(podpis Administratora)

Przyjmuję do wiadomości i stosowania.

.....
(Podpis osoby upoważnionej)

Garwolin, dnia r.

.....
(pieczęć Szkoły)

**ODWOŁANIE UPOWAŻNIENIA nr ...
do przetwarzania danych osobowych**

Odwołuję z dniem upoważnienie nr/20....
do przetwarzania danych osobowych wystawione dla Pani/Pana

Administrator

.....
(pieczętka i podpis)

Garwolin, dnia r.

.....
(pieczęć Szkoły)**EWIDENCJA OSÓB UPOWAŻNIONYCH
DO PRZETWARZANIA DANYCH OSOBOWYCH**

Nr upoważnienia	Nazwisko i imię	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data odebrania uprawnień	Uwagi

Garwolin, dnia r.

.....
(imię i nazwisko)

.....
(stanowisko)

OŚWIADCZENIE

o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Szkole zasadach dotyczących przetwarzania danych osobowych, określonych w „Polityce ochrony danych osobowych przetwarzanych w Katolickim Liceum Ogólnokształcącym im. C. K. Norwida” i zobowiązuję się ich przestrzegać. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w Szkole.

Zostałem/am zapoznany/a z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE L 119, s. 1) i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Poinformowano mnie również o grożącej, stosownie do przepisów rozdziału 8 ustawy o ochronie danych osobowych odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że złamanie zasad ochrony danych osobowych, obowiązujących w Katolickim Liceum Ogólnokształcącym im. C. K. Norwida może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

.....
(podpis pracownika)

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

I. 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 Szkole.
2. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ASI.
3. ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez Administratora.
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.

II. Zabezpieczenie danych w systemie informatycznym

1. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.
2. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.
3. 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) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
 - d) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
 - e) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
4. 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.
5. 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.
 6. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

III. Zasady bezpieczeństwa podczas pracy w systemie informatycznym

1. W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
 - 1) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła (autoryzacja użytkownika w bazie usług katalogowych),
 - 2) 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 systemu 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 przetwarzane dane;
 - d) stwierdzenia użytkownika 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.

IV. Tworzenie kopii zapasowych

1. Pełne kopie zapasowe zbiorów danych tworzone są 4 razy w ciągu roku. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.
2. Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane.
3. Kopie przechowywane są w szafie metalowej w sekretariacie Szkoły.
4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. 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.

V. Przeglądy i konserwacje systemów

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych przedstawicieli wykonawców.
2. Prace wymienione w pkt 1 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3. Przed rozpoczęciem prac wymienionych w pkt 1 przez osoby niebędące pracownikami Szkoły należy dokonać potwierdzenia tożsamości tychże osób.

VI. 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 / w sposób uniemożliwiający ich odczytanie (pocięte w poprzeczne paski).
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 w niszczarce.

Zasady
postępowania w przypadku wykrycia naruszenia ochrony danych osobowych
przetwarzanych w Katolickim Liceum Ogólnokształcącym im. C. K. Norwida

1. Cel

W niniejszym dokumencie ustalone zostały zasady analizowania przypadków dotyczących naruszenia ochrony danych osobowych oraz sposób postępowania przy zgłaszaniu naruszenia ochrony danych osobowych w myśl przepisów art. 33 i art. 34 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119/1, z 4 maja 2016 r.).

2. Definicje

Ilekość w niniejszej instrukcji zostanie użyte pojęcie:

- 1) Szkołę – należy przez to rozumieć Katolickie Liceum Ogólnokształcące im. C. K. Norwida w Garwolinie;
- 2) Dyrektor – należy przez to rozumieć Dyrektora Szkoły;
- 3) RODO – należy przez to rozumieć 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 (Dz. Urz. UE L 119/1, z 4 maja 2016 r.);
- 4) dane osobowe – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- 5) naruszenie ochrony danych osobowych – należy przez to rozumieć, każdą sytuację która jest wynikiem zdarzeń losowych lub działania sił natury bądź nieumyślnego lub celowego działania człowieka i powoduje lub może spowodować zagrożenie bezpieczeństwa danych osobowych przetwarzanych w Szkole.

3. Zakres stosowania

Instrukcja obowiązuje wszystkich pracowników Szkoły i dotyczy zidentyfikowanych przypadków zagrażających bezpieczeństwu danych osobowych przetwarzanych w Szkole, zarówno w formie papierowej, jaki i przy wykorzystaniu systemów teleinformatycznych.

4. Odpowiedzialność

- 1) Każda osoba zatrudniona w Szkole lub wykonująca prace na rzecz Szkoły (stażysta, praktykant, przedstawiciel podmiotu zewnętrznego współpracujący ze Szkołą) jest zobowiązana do niezwłocznego zgłoszenia faktu wykrycia przypadków mających znaczenie dla prawidłowego funkcjonowania Szkoły.

- 2) Obsługę zgłoszonych przypadków związanych z naruszeniem bezpieczeństwa danych osobowych zapewnia wicedyrektor szkoły.
- 3) Punkt kontaktowy do zgłaszania przypadków związanych z naruszeniem bezpieczeństwa danych osobowych:
 - pokój wicedyrektora
 - tel. 25 6823700
 - adres e-mail: magofka@poczta.onet.pl

5. Tryb postępowania

5.1. Wykrycie sytuacji naruszenia bezpieczeństwa danych osobowych.

- 1) Sytuacje, które będą związane z naruszeniem bezpieczeństwa danych osobowych odnoszą się do:
 - utraty danych (kradzież, zgubienie, zniszczenie danych),
 - przekazania danych osobie lub podmiotowi nieuprawnionemu na skutek działania umyślnego lub w wyniku błędu pracowników lub współpracowników Szkoły.
- 2) W przypadku wykrycia naruszenia bezpieczeństwa danych osobowych należy, o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, oraz uwzględnić w działaniu również ustalenie przyczyn lub sprawców. W szczególności należy:
 - rozważyć wstrzymanie bieżącej pracy w celu zabezpieczenia miejsca zdarzenia (wylogować się z systemu, wyłączyć urządzenie);
 - zaniechać, o ile to możliwe, dalszych działań, które wiążą się z zaistniałą sytuacją i mogą utrudnić jej udokumentowanie i późniejszą analizę;
 - w zależności od okoliczności zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałej sytuacji (np. zasady BHP, ewakuacja z budynku, procedury ppoż.),
 - poinformować wicedyrektora szkoły wg zasad określonych w niniejszym dokumencie.

5.2. Zgłaszanie sytuacji naruszenia bezpieczeństwa danych osobowych.

- 1) Z uwagi na wymogi wynikające z RODO, w tym krótki okres na zgłoszenie naruszenia bezpieczeństwa danych osobowych (72 godziny od stwierdzenia/wykrycia naruszenia) informacje w tym zakresie muszą być przekazywane przez osoby, które zidentyfikowały zagrożenie, bez zbędnej zwłoki.
- 2) Wykrycia naruszenia lub podejrzenie wystąpienia zdarzenia, które może mieć wpływ na bezpieczeństwo przetwarzanych danych należy zgłosić do wicedyrektora szkoły.
- 3) Zgłoszenie musi zawierać miejsce wystąpienia naruszenia bezpieczeństwa danych osobowych oraz, w miarę możliwości, jego krótki opis.

5.3. Analiza przypadków naruszenia bezpieczeństwa danych osobowych.

- 1) Każdy zgłoszony przypadek musi zostać poddany analizie, w zakresie ustalenia czy faktycznie doszło do naruszenia bezpieczeństwa danych osobowych, a w szczególności analiza powinna dać możliwość ustalenia czy doszło do naruszenia

bezpieczeństwa danych osobowych, które może skutkować ryzykiem naruszenia praw i wolności osób, np. jeśli naruszenie może prowadzić do kradzieży lub fałszowania tożsamości, straty finansowej, naruszenia dobrego imienia czy też naruszenia tajemnic prawnie chronionych.

- 2) W trakcie analizy należy brać pod uwagę następujące elementy:
 - wdrożone zabezpieczenia i ich funkcjonowanie (potwierdzenie ich skuteczności),
 - zapisy (logi systemowe/rejestry) systemu teleinformatycznego, jeśli zachodzi podejrzenie utraty poufności przetwarzanych danych (np. kradzież danych z bazy),
 - poprawność funkcjonowania systemu – bazy danych jeśli zachodzi podejrzenie utraty integralności przetwarzanych danych (np. uszkodzenie bazy danych),
 - zapisy (logi systemowe/nagrania/rejestry) systemów zabezpieczeń wspomagających ochronę systemów teleinformatycznych oraz przetwarzanych danych, jeśli zachodzi podejrzenie nieautoryzowanego dostępu do danych.
- 3) Analiza przeprowadzana jest przez wicedyrektora szkoły.
- 4) O wystąpieniu sytuacji naruszenia bezpieczeństwa danych osobowych przetwarzanych w Szkole jest informowany Dyrektor.

5.4. Zawiadomienie organu nadzorczego o sytuacji naruszenia bezpieczeństwa danych osobowych.

- 1) Jeżeli przeprowadzona analiza, o której mowa w podrozdziale 5.3 wskazuje na naruszenie bezpieczeństwa danych osobowych, które może skutkować ryzykiem naruszenia praw i wolności osób, informacja o tym zdarzeniu jest kierowana do Urzędu Ochrony Danych Osobowych.
- 2) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonywane jest w sposób określony przez organ nadzorczy nie później niż 72 godziny od stwierdzenia (wykrycia) zdarzenia.
- 3) Jeżeli zgłoszenie naruszenia bezpieczeństwa danych osobowych dokonane zostanie po upływie 72 godzin od stwierdzenia (wykrycia) zdarzenia, musi ono zawierać wyjaśnienie przyczyn opóźnienia.
- 4) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonuje wicedyrektor.

5.5. Zawiadomienie osoby, której dane dotyczą o sytuacji naruszenia bezpieczeństwa jej danych osobowych.

- 1) Jeżeli przeprowadzona analiza, o której mowa w podrozdziale 5.3 wskazuje na naruszenie bezpieczeństwa danych osobowych, które może skutkować wysokim ryzykiem naruszenia praw i wolności osób, informacja o tym zdarzeniu jest kierowana bez zbędnej zwłoki do osób których dane dotyczą.
- 2) Zawiadomienia o naruszeniu, powinno zawierać opis jego charakteru naruszenia, możliwe konsekwencje dla osób których dane dotyczą oraz możliwe do zastosowania środki zalecane w celu poradzenia sobie z naruszeniem i zminimalizowania jego negatywnych skutków.
- 3) Zawiadomienia o naruszeniu powinno zostać przekazane zainteresowanym osobom, biorąc pod uwagę dostępne kanały komunikacji z nimi oraz koszty wysyłki korespondencji np. z uwagi na liczbę osób objętych zawiadomieniem:

- na adres e-mail (jeśli znany),
 - telefonicznie (jeśli znany nr telefonu),
 - listownie (jeśli znany adres).
- 4) Zawiadomienie w formie, o której mowa w pkt 2, nie jest wymagane, jeśli:
- w celu zabezpieczenia danych wprowadzone zostały w Szkole rozwiązania uniemożliwiające odczyt osobom nieuprawnionym dostępu do tych danych (np. zaszyfrowanie danych),
 - zostały wprowadzone środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osób.
- 5) Bezpośrednie zawiadomienie nie jest również wymagane, jeśli podawałoby to poniesienie niewspółmiernie dużych nakładów pracy i środków finansowych ze strony Szkoły.
- 6) W przypadku zaistnienia sytuacji, o której mowa w pkt 5, należy wydać publiczny komunikat (informacja na stronie Biuletynu Informacji Publicznej Szkoły, jednorazowe ogłoszenie w dzienniku o zasięgu regionalnym).
- 5.6. Usuwanie naruszenia bezpieczeństwa danych osobowych
- 1) W usuwanie naruszenia bezpieczeństwa danych osobowych zaangażowani są pracownicy Szkoły, którzy w ramach powierzonych obowiązków zapewniają i nadzorują funkcjonowanie systemu zabezpieczeń danych osobowych.
 - 2) Po wykryciu naruszenia bezpieczeństwa danych osobowych analizowane są okoliczności związane z jego wystąpieniem oraz ustalany jest sposób rozwiązania problemu oraz, jeśli to konieczne, zabezpieczeniu materiału dowodowego.
 - 3) W przypadku gdy problem może zostać rozwiązany samodzielnie przez pracowników Szkoły, należy to wykonać bez zbędnej zwłoki.
 - 4) W przypadku konieczności wykonania działań przez podmiot zewnętrzny, pracownik zajmujący się rozwiązaniem problemu powinien, używając ustalonych metod, poinformować o zdarzeniu ten podmiot, oraz razem z jej przedstawicielem uczestniczyć w rozwiązywaniu problemu.
 - 5) W przypadku wykrycia działań umyślnych pracownik odpowiedzialny za obsługę naruszenia bezpieczeństwa danych osobowych przekazuje wyniki analizy, wraz z zabezpieczonym materiałem dowodowym, Dyrektorowi w celu wyciągnięcia konsekwencji dyscyplinarnych wobec pracownika Szkoły lub podjęcia kroków prawnych wobec osób trzecich.
 - 6) Po przywróceniu prawidłowego stanu bezpieczeństwa danych osobowych należy przeprowadzić analizę w celu określenia przyczyny naruszenia oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
 - 7) Jeżeli przyczyną naruszenia bezpieczeństwa danych osobowych:
 - był błąd osoby przetwarzającej dane, w szczególności użytkownika systemu teleinformatycznego, można przeprowadzić dodatkowe szkolenie lub przesłać stosowną informację do wszystkich użytkowników systemu o sposobie postępowania przy przetwarzaniu danych osobowych oraz zapewnieniu ich bezpieczeństwa;

- było uaktywnienie złośliwego kodu, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe;
 - było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje służbowe;
 - było włamanie lub uszkodzenie systemu zabezpieczeń w celu pozyskania danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony danych osobowych;
 - był zły stan urządzeń lub sposób działania oprogramowania, należy niezwłocznie przeprowadzić kontrolne czynności serwisowe.
- 8) Do celów dowodowych, naruszenie bezpieczeństwa danych osobowych może zostać dodatkowo szczegółowo udokumentowane.

6. Załączniki

Załącznik nr 1. Wzór „Raportu o naruszeniu danych osobowych”

Załącznik nr 2. Wzór „Zawiadomienia o naruszeniu danych przesyłanego do osób których dane zostały naruszone”

do „Zasad postępowania w przypadku wykrycia naruszenia ochrony danych osobowych przetwarzanych w Katolickim Liceum Ogólnokształcącym im. C. K. Norwida”

Wzór „Raportu o naruszeniu danych osobowych”

1. Opis naruszenia ochrony danych osobowych

W dniu zidentyfikowano naruszenie ochrony danych osobowych w zakresie ujawnienia (wskazać rodzaj danych osobowych):

-

-

-

2. Kategoria i przybliżona liczba osób/wpisów danych których dotyczy naruszenie

.....
.....
.....

3. Możliwe konsekwencje naruszenia ochrony danych osobowych

.....
.....
.....

4. Opis środków zastosowanych lub proponowanych do zastosowania w celu zaradzenia naruszeniu ochrony danych osobowych

.....
.....
.....

do „Zasad postępowania w przypadku wykrycia naruszenia ochrony danych osobowych przetwarzanych w Katolickim Liceum Ogólnokształcącym im. C. K. Norwida”

Wzór „Zawiadomienia o naruszeniu danych osobowych”

Informuję, że w wyniku w dniu doszło do naruszenia Pani/Pana danych osobowych w zakresie ujawnienia (wskazać rodzaj danych osobowych):

-

-

-

Naruszenie zostało spowodowane (włamaniem i kradzieżą danych z bazy/nieprawidłowym przesłaniem danych przez pracownika/)

W związku z powyższym istnieje duże ryzyko kradzieży lub sfalszowania Pani/Pana tożsamości, co może spowodować stratę finansową lub utratę dobrego imienia w przypadku wykorzystania tych danych przez osoby nieuprawnione w sposób niezgodny z prawem.

Informacja dotycząca kradzieży danych została zgłoszona do organów ścigania

W celu zminimalizowania negatywnych skutków tego naruszenia należy zastrzec dowód tożsamości/zmienić hasło/.....

Dodatkowe informacje w tym zakresie można uzyskać:

- pod nr telefonu

- wysyłając zapytanie na adres e-mail:

.....

podpis Dyrektora