……..

DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH

Liceum Ogólnokształcącego im. Stefana Żeromskiego w Bartoszycach

Aktualizacja 01.03.2021

SPIS TREŚCI

WPROWADZENIE

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich ochrony w Liceum Ogólnokształcącym im. Stefana Żeromskiego z siedzibą przy ul .Bohaterów Monte Cassino 9 11-200 Bartoszyce, zwanym dalej **SZKOŁĄ.**

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym wyrażone w Polityce bezpieczeństwa oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Wszelkie zestawienia uzupełniające treść dokumentu zebrano w postaci załączników. Do najważniejszych należy ewidencja zbiorów osobowych, miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych, a także lista środków organizacyjnych i technicznych służących bezpieczeństwu danych.

1.1. PODSTAWY PRAWNE

Przepisy ochrony danych osobowych zawarte są w ustawie o ochronie danych osobowych oraz wydanych do niej aktach wykonawczych. Pełną listę aktów prawnych stanowią:

Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

USTAWA z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000).

1.2. DEFINICJE

W dokumencie przyjmuje się następującą terminologię:

Prezes Urzędu Ochrony Danych Osobowych – organ do spraw ochrony danych osobowych.

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Dane wrażliwe - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, 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. Dane genetyczne oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej. Dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Dane dotyczące zdrowia oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

Administrator danych osobowych (ADO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. ADO w szkole jest **Dyrektor**.

Inspektor ochrony danych (IOD) – osoba nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

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

Przetwarzanie danych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Ograniczenie przetwarzania - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

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 – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

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

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

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

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

NAJWAŻNIEJSZE ZAGADNIENIA OCHRONY DANYCH OSOBOWYCH

2.1. DEFINICJA POLITYKI BEZPIECZEŃSTWA

Polityka bezpieczeństwa przetwarzania danych osobowych w Liceum Ogólnokształcącym im. Stefana Żeromskiego w Bartoszycach, zwana dalej „Polityką bezpieczeństwa", określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie przetwarzania danych osobowych.

2.2. PRZETWARZANIE DANYCH

Przetwarzanie danych jest **dopuszczalne** tylko wtedy gdy:

Osoba, której dane dotyczą, **wyrazi na to zgodę**, chyba że chodzi o usunięcie dotyczących jej danych. Zgoda może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. Zgoda nie może być domniemana lub dorozumiana. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie zgody nie jest możliwie, można przetwarzać

dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.

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 Administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Za prawnie usprawiedliwiony cel uważa się w szczególności: marketing bezpośredni własnych produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Przetwarzanie danych jest **zabronione** w przypadku 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 tych danych **jest jednak dopuszczalne**, jeżeli:

osoba, której dane dotyczą, **wyrazi na to zgodę na piśmie**, chyba że chodzi o usunięcie dotyczących jej danych,

przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,

przetwarzanie takich danych jest **niezbędne do ochrony żywotnych interesów osoby**, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

jest to niezbędne do wykonania **statutowych zadań kościołów i innych związków wyznaniowych**, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,

przetwarzanie dotyczy danych, które są niezbędne **do dochodzenia praw przed sądem**,

przetwarzanie jest **niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób**, a zakres przetwarzanych danych jest określony w ustawie,

przetwarzanie jest prowadzone **w celu ochrony stanu zdrowia**, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

przetwarzanie dotyczy danych, które zostały podane **do wiadomości publicznej przez osobę**, której dane dotyczą,

jest to niezbędne do **prowadzenia badań naukowych**, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,

przetwarzanie danych jest prowadzone przez stronę **w celu realizacji praw i obowiązków wynikających z orzeczenia** wydanego w postępowaniu sądowym lub administracyjnym.

2.3. OBOWIĄZKI INFORMACYJNE O PRZETWARZANIU DANYCH

Zbieranie danych osobowych od osób, których dane dotyczą

W przypadku zbierania danych od osoby, której te dane dotyczą Administrator danych jest zobowiązany poinformować tę osobę o:

- adresie swojej siedziby i pełnej nazwie,

- celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

- prawie dostępu do treści swoich danych oraz ich poprawiania,

- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

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

Zbieranie danych osobowych nie od osób, których dane dotyczą.

W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator danych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu danych o:

- adresie swojej siedziby i pełnej nazwie,

- celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,

- źródle danych,

- prawie dostępu do treści swoich danych oraz ich poprawiania,

- prawie wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,

- prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy Administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Podanych wyżej zasad **nie stosuje się**, jeżeli:

- dane są przetwarzane przez administratora na podstawie przepisów prawa,

- przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,

- dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania.

2.4. UDOSTĘPNIANIE DANYCH

Najważniejsze przesłanki i zasady udostępniania danych.

Nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie.

Nie ma znaczenia (ujmując problem technicznie) czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd.

Udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa.

Dane osobowe, z wyłączeniem danych wrażliwych, mogą być udostępniane nie w oparciu o przepisy prawa, jeżeli osoba wnioskująca w sposób wiarygodny uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

2.5. POWIERZENIE PRZETWARZANIA DANYCH

W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla Administratora danych może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami:

- Umowa powinna być zawarta niezależnie od posiadanej umowy określającej relacje obu stron,

- Podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianym w umowie,

- Podmiot, któremu powierzono przetwarzanie danych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych,

- Odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na Administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową. do kontroli zgodności przetwarzania danych przez podmiot, któremu powierzono przetwarzanie danych.

2.6. DOKUMENTOWANIE

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do **zagrożeń** oraz **kategorii danych** objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Ponadto, Administrator danych:

- prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki organizacyjne i techniczne służące ochronie danych,

- wyznacza **inspektora ochrony danych**, nadzorującego przestrzeganie zasad ochrony,

- nadaje **upoważnienia do przetwarzania danych** i dopuszcza do pracy wyłącznie osoby posiadające takie upoważnienie,

- zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,

- prowadzi ewidencję osób upoważnionych do ich przetwarzania, która zawiera: imię i nazwisko osoby upoważnionej, datę zapoznania z dokumentem, stanowisko/funkcję, typ umowy, zakres rzeczowy oraz ramy czasowe przetwarzania.

2.7. SANKCJE KARNE

Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie **nie jest dopuszczalne** albo do których przetwarzania **nie jest uprawniony**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **lat dwóch**.

Jeżeli czyn ten dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **lat trzech**.

Kto **udaremnia lub utrudnia kontrolującemu prowadzenie kontroli** przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **lat dwóch**

Kto administrując zbiorem danych przechowuje w zbiorze dane osobowe **niezgodnie z celem utworzenia zbioru**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.

Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych **udostępnia je lub umożliwia dostęp** do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **lat dwóch**. Jeżeli sprawca działa **nieumyślnie**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.

Kto administrując danymi **narusza choćby nieumyślnie obowiązek zabezpieczenia** ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.

Kto administrując zbiorem danych **nie dopełnia obowiązku poinformowania osoby, której dane dotyczą**, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.

Wobec osoby, która w przypadku naruszenia zasad bezpieczeństwa lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonych w niniejszej dokumentacji, a w szczególności nie powiadomiła

odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, **wszczyna się postępowanie dyscyplinarne**.

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie **obowiązków pracowniczych**.

Prezes Urzędu może nałożyć na podmiot obowiązany do przestrzegania przepisów rozporządzenia 2016/679 w drodze decyzji, **administracyjną karę pieniężną** w wysokości do **10 000** złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

ZAGROŻENIA BEZPIECZEŃSTWA

3.1. 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.

3.2. SYTUACJE ŚWIADCZĄCE O NARUSZENIU ZASAD BEZPIECZEŃSTWA

Przełamane zabezpieczenia tradycyjnych – niezamknięcie drzwi na klucz lub pozostawienie pomieszczenia bez opieki,

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

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, a w tym 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 (autoryzacji),

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 lub jego sieci komputerowej 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.

ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,

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

rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3.3. TABELE FORM NARUSZENIA BEZPIECZEŃSTWA I SPOSOBY POSTĘPOWANIA

Tabela form naruszenia ochrony danych osobowych przez osoby zatrudnione przy przetwarzaniu danych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić inspektora danych osobowych.
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić inspektora danych osobowych. Sporządzić raport.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić inspektora danych osobowych. Sporządzić raport.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Sporządzić raport.
Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.
W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport.

Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestania kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić inspektora danych osobowych. Sporządzić raport.
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić inspektora danych osobowych. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć pomieszczenie. Powiadomić przełożonych. Sporządzić raport.
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i inspektora danych osobowych. Sporządzić raport.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i inspektora danych osobowych. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i inspektora danych osobowych. Sporządzić raport.
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i inspektora danych osobowych. Sporządzić raport.

Tabela zjawisk świadczących o możliwości naruszenia ochrony danych osobowych

FORMY NARUSZEŃ

SPOSOBY POSTĘPOWANIA

Ślady manipulacji przy układach sieci komputerowej lub komputerach.

Powiadomić niezwłocznie inspektora ochrony danych oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. **Sporządzić raport.**

Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.
Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. **Sporządzić raport**.

Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.

Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.

Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.

Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.

Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie inspektora danych osobowych.
Sporządzić raport.

Tabela naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	**Powiadomić inspektora danych osobowych. Sporządzić raport.**
Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	

POLITYKA BEZPIECZEŃSTWA

Polityka bezpieczeństwa rozumiana jest jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Instytucji. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

4.1. DEKLARACJA

Administrator danych mając świadomość, iż przetwarza dane **wrażliwe** uczniów deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.

W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumenty te są uzupełniane załącznikami do dokumentacji, na które składają się m.in.: wykazy zbiorów, miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych.

W celu zapewnienia prawidłowego monitorowania przetwarzania danych wprowadza się liczne ewidencje, które szczegółowo charakteryzują obszary objęte monitoringiem, umożliwiając pełną kontrolę nad tym, jakie dane i przez kogo są przetwarzane oraz komu udostępniane.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

4.2. CHARAKTERYSTYKA INSTYTUCJI

Szkoła realizuje zadania głównie na mocy przepisów prawa zawartych w Ustawie. Prawo oświatowe, systemie informacji oświatowej oraz Karcie Nauczyciela, a także innych aktach wykonawczych uprawniających Dyrektora szkoły do podejmowania stosownych działań, w tym do przetwarzania danych osobowych. Podstawowym obszarem działania są zadania związane z bezpłatnym nauczaniem.

4.3. ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

Przetwarzanie danych osobowych w Szkole może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.

Administrator danych **powołuje Inspektora ochrony danych.**

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne **upoważnienie**. Wzór upoważnienia stanowi **załącznik nr 2** do niniejszej dokumentacji.

IOD prowadzi **ewidencję osób upoważnionych,** która zawiera: imię i nazwisko osoby upoważnionej, datę zapoznania z dokumentem, stanowisko/funkcję, typ umowy, zakres rzeczowy oraz ramy czasowe przetwarzania.

Stanowi ona **załącznik nr 3**. Na jej podstawie przygotowuje **Upoważnienia do przetwarzania danych** i przedkłada je do podpisu ADO.

Unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego **załącznik nr 4** do niniejszej dokumentacji.

Każdy pracownik Szkoły co najmniej raz na 2 lata musi odbyć **szkolenie z zakresu ochrony danych** osobowych. Za organizację szkoleń odpowiedzialny jest IOD, który prowadzi w tym celu odpowiednią dokumentację. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.

Ponadto każdy upoważniony do przetwarzania danych **potwierdza pisemnie** fakt odbycia szkolenia, zapoznania się z niniejszą dokumentacją, zrozumienia wszystkich zasad bezpieczeństwa oraz zachowania poufności. Wzór oświadczenia stanowi **załącznik nr 5** do niniejszej dokumentacji. Podpisany dokument jest dołączany do akt osobowych i dokumentacji inspektora.

Pracownicy, którzy nie przetwarzają danych osobowych, podpisują oświadczenie o zachowaniu poufności (**załącznik nr 6**).

Dane osobowe gromadzone i przetwarzane są w budynku Liceum Ogólnokształcącego im Stefana Żeromskiego w Bartoszycach pod adresem: ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce. Obszar przetwarzania danych osobowych określony w **załączniku nr 1** do niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.

Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. Stosuje się zasadę „czystego pulpitu" – dokumenty z danymi osobowymi powinny być zapisane na dysku D (jeżeli komputer posiada partycje) lub w Moich Dokumentach.

Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.

Przetwarzanie danych podawanych dobrowolnie, które mają służyć promowaniu działalności szkoły oraz wykorzystanie wizerunku ucznia może odbywać się tylko na podstawie pisemnej zgody podającego te dane wg wzoru określonego w **załączniku nr 8 i nr 9**.

Przetwarzanie danych osobowych oraz wykorzystanie wizerunku ucznia uczestniczącego w zawodach sportowych/konkursach przedmiotowych/olimpiadach etc. może odbywać się tylko na podstawie pisemnej zgody podającego te dane wg wzoru określonego w **załączniku nr 10**.

Dla zapewnienia kontroli przestrzegania zasad określonych w niniejszej dokumentacji wyznacza się następujące **zadania Inspektorowi ochron danych:**

Nadzór nad przetwarzaniem danych zgodnie z ustawą o ochronie danych osobowych i innymi przepisami prawa.

Kontrola przestrzegania zasad ochrony – systematycznie, nie rzadziej niż dwa razy do roku kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w szczególności:

1. Kontrola dokumentacji opisującej sposób przetwarzania oraz ochrony.
2. Kontrola fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są informacje.
3. Kontrola poprawności zabezpieczeń danych przetwarzanych metodami tradycyjnymi.
4. Kontrola awaryjnego zasilania komputerów.

5. Nadzór nad naprawą, konserwacją oraz likwidacją urządzeń komputerowych.
6. Kontrola systemu kontroli obecności wirusów komputerowych.
7. Kontrola wykonywania kopii awaryjnych.
8. Kontrola przeglądu, konserwacji oraz uaktualnienia systemów informatycznych.
9. Kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych.
10. Kontrola nadanych upoważnień.

Przedstawianie Administratorowi danych wyników kontroli.

Systematyczna analiza dokumentacji pod kątem obszarów, zbiorów oraz zasad ochrony.

Szkolenie z ochrony danych osobowych oraz aktów wykonawczych.

Podjęcie natychmiastowych działań zabezpieczających w przypadku otrzymania informacji o naruszeniu bezpieczeństwa informacji.

Prowadzenie monitoringu przetwarzania danych.

Każdorazowe sporządzenie raportu zgodnie ze wzorem będącym **załącznikiem nr 7** do niniejszej dokumentacji oraz przedstawienie efektów działań Administratorowi danych.

4.4. ŚRODKI TECHNICZNE OCHRONY DANYCH OSOBOWYCH

Zbiory danych przetwarzane w Szkole zabezpiecza się poprzez:

1. Środki ochrony fizycznej.

Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi) zamykanymi na klucz.

Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych mają tylko osoby upoważnione.

Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej metalowej szafie.

Zbiory danych osobowych w formie elektronicznej przechowywane są na serwerach firmy Librus (podpisana umowa), które są zabezpieczone w sposób przewidziany prawem.

Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi) zamykanymi na klucz dodatkowo zabezpieczone kratą zamykaną na klucz.

Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej metalowej szafie.

Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

2. Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej.

Zbiory danych osobowych przetwarzane są przy użyciu komputerów stacjonarnych i przenośnych.

Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła, które musi składać się z minimum 8 znaków. Hasło musi być zmieniane raz na miesiąc. Komputery dyrektora, wicedyrektora, sekretariatu i pedagoga są zabezpieczane hasłem składającym się z 8 znaków zawierających małe, wielkie litery, cyfry oraz znaki specjalne.

Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.

Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.

Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

Użyto system Firewall do ochrony dostępu do sieci komputerowej.

3. Środki ochrony w ramach systemowych narzędzi programowych i baz danych.

Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych.

Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanych zbiorów danych osobowych.

Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych.

Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określa **Instrukcja zarządzania systemem informatycznym** służącym do przetwarzania danych osobowych opisana w pkt 6 niniejszej dokumentacji.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

I. *CHARAKTERYSTYKA SYSTEMU*

Sieć informatyczna ma strukturę gwiazdy, ze switchami, do których podłączone są komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.

1. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.
2. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku .

II. *OGÓLNE ZASADY PRACY W SYSTEMIE INFORMATYCZNYM*

1. IOD oraz administrator odpowiadają za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.
2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez administratora do eksploatacji licencjonowane oprogramowanie.
3. Administrator prowadzi ewidencję oprogramowania.
4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:

   - mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu,

   - mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej,

   - na wyznaczonych komputerach mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,

   - mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,

   - mechanizmy zarządzania zmianami.

5. **Użytkownikom zabrania się:**

   - korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy Szkoły bez pisemnej zgody ADO,

   - udostępniania stanowisk roboczych osobom nieuprawnionym,

   - wykorzystywania sieci komputerowej Szkoły w celach innych niż wyznaczone przez ADO,

   - samowolnego instalowania i używania programów komputerowych,

   - korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,

   - umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej Szkoły oraz sieci Internetowej osobom nieuprawnionym,

   - używania komputera bez zainstalowanego oprogramowania antywirusowego.

III. *PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI.*

1. Użytkowników systemu informatycznego tworzy oraz usuwa administrator na podstawie zgody ADO.
2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
3. Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi załącznik nr 3 do niniejszej dokumentacji.
4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:
    a. nieobecności pracownika w pracy trwającej dłużej niż 31 dni kalendarzowych,
    b. zawieszenia w pełnieniu obowiązków służbowych.
5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

IV. *STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.*

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator nadany przez administratora.
3. W identyfikatorze pomija się polskie znaki diakrytyczne.
4. Hasło składa się z co najmniej ośmiu znaków (u nauczycieli), zawiera co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny (u dyrektora, wicedyrektora, pracowników sekretariatu i pedagoga).
5. Zmianę hasła należy dokonywać nie rzadziej niż co 30 dni.
6. Hasła użytkowników generuje administrator i zobowiązuje użytkownika do jego zmiany przy pierwszym zalogowaniu. Hasło nie może być zapisywane i przechowywane.
7. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

V. *PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY.*

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.
3. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.

4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3.
5. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.
6. ABI monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

VI. *PROCEDURY TWORZENIA KOPII AWARYJNYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA.*

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.
2. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
3. Zabezpieczeniu poprzez wykonywanie kopii awaryjnych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
4. Za proces tworzenia kopii awaryjnych odpowiada administrator.
5. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, użytkownicy systemu informatycznego zobowiązani są do wykonywania samodzielnie kopii bezpieczeństwa tych zbiorów.
6. Kopie awaryjne mogą być wykonywane tylko na nośnikach informatycznych dostarczonych przez administratora.
7. Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
8. Kopie awaryjne wykonuje się okresowo według potrzeb poszczególnych użytkowników
9. Kopie awaryjne przechowuje administrator, a w przypadku przetwarzania danych na stacjach roboczych poszczególni użytkownicy. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności.
10. ABI zobowiązany jest do okresowego wykonywania testów odtworzeniowych kopii awaryjnych.
11. Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, zaś po upływie czasu ich przydatności – niszczone w niszczarkach dokumentów.

VII. *SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI.*

1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu informatycznego, przechowuje ABI w odpowiednio zabezpieczonym pomieszczeniu.
2. W uzasadnionych przypadkach, za zgodą ABI, dane osobowe można przetwarzać na dyskach twardych komputerów stacjonarnych lub zarejestrowanych nośnikach informacji dostarczonych przez administratora.
3. Przenośne nośniki danych powinny być zabezpieczone ochroną kryptograficzną.
4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a. **likwidacji** — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

b. **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

c. **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem administratora.

5. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym przez administratora.

VIII. *SPOSÓB ZABEZPIECZENIA SYSTEMU PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO.*

1. ABI zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody. System antywirusowy jest skonfigurowany w następujący sposób:
   a. skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.
   b. automatycznej aktualizacji wzorców wirusów.
2. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie administratora.
3. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, administrator podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
   a. usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
   b. odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
   c. samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.
4. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
5. ABI monitoruje stan systemu, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system.

IX. *INFORMACJE O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPNIONE, DACIE I ZAKRESIE TEGO UDOSTĘPNIENIA.*

1. Informacje o udostępnieniu danych osobowych przetwarza się i przechowuje w oparciu o Rzeczowy Wykaz Akt i Instrukcję kancelaryjną.
2. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest ADO.
3. Nadzór nad właściwym udostępnianiem danych prowadzi administrator.

X. *PRZESYŁANIE DANYCH POZA OBSZAR PRZETWARZANIA*

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.
2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:
    a. zatwierdzenie przez administratora zakresu danych osobowych przeznaczonych do wysłania,
    b. zastosowanie mechanizmów szyfrowania danych osobowych,
3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.
4. ABI tworzy konfigurację mechanizmów kryptograficznych w sposób:
    a. zapewniający wykorzystanie obowiązujących wymagań w zakresie kryptograficznej ochrony danych osobowych,
    b. umożliwiający, w miarę technicznych możliwości, automatyczne szyfrowanie danych osobowych wysyłanych poza obszar przetwarzania danych,
    c. informujący użytkownika o dołączeniu do wysyłanych danych osobowych elektronicznego podpisu i wymagający przed wysłaniem informacji potwierdzenia podpisywanej treści.
5. Administrator bezpieczeństwa informacji jest odpowiedzialny za realizację procesów związanych z zarządzaniem aplikacjami kryptograficznymi oraz generowanie kluczy dostępowych do tych aplikacji.

XI. *PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH.*

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO.
2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez administratora.
3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez administratora.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza Szkołą, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.
5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.
6. ABI wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

6. ZAŁĄCZNIKI

Załącznik nr 1. Obszary przetwarzania danych osobowych w Szkole.

Załącznik nr 2a, b, c, d. Wzory upoważnień do przetwarzania danych osobowych.

Załącznik nr 3. Wzór ewidencji osób upoważnionych do przetwarzania danych.

Załącznik nr 4. Wzór unieważnienia upoważnienia do przetwarzania danych.

Załącznik nr 5. Wzór oświadczenia o zapoznaniu się z dokumentacją, jej zrozumieniem oraz zachowaniem poufności.

Załącznik nr 6. Wzór oświadczenia o zachowaniu poufności przez pracowników obsługi.

Załącznik nr 7. Wzór raportu z przeprowadzonej kontroli przez inspektora danych osobowych.

Załącznik nr 8. Zgoda rodzica na wykorzystanie danych osobowych /wizerunku dziecka w celu promowania szkoły i informowaniu o jej działalności.

Załącznik nr 9. Zgoda pełnoletniego ucznia na wykorzystanie danych osobowych/wizerunku w celu promowania szkoły i informowaniu o jej działalności.

Załącznik nr 10. Zgoda rodzica/ucznia na wykorzystanie danych osobowych/wizerunku w celu uczestniczenia w zawodach/konkursach/olimpiadach.

Załącznik nr 11. Lista osób, które zapoznały się z Dokumentacją ochrony danych Liceum Ogólnokształcącego im. Stefana Żeromskiego w Bartoszycach

ZAŁĄCZNIK NR 1. OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE

Lp.	Nazwa pomieszczenia	Adres
Liceum Ogólnokształcące im. Stefana Żeromskiego w Bartoszycach		
1	Sekretariat	*ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce*
2	Gabinet Dyrektora	*ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce*
3	Gabinet Wicedyrektora	*ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce*
4	Biblioteka	*ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce*
5	Gabinet pedagoga szkolnego	*ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce*
6	Pokój nauczycielski	*ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce*
7	Sale lekcyjne	*ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce*
8	Księgowość 5a	*ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce*
9	Gabinet pielęgniarki	*ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce*

ZAŁĄCZNIK NR 2A. WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH (IOD)

Bartoszyce, dnia .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

UPOWAŻNIENIE nr ..... z dn. .....
obowiązuje od .....

Na podstawie art. 29 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO** oraz w związku z powierzeniem funkcji **Inspektora Ochrony Danych Osobowych**, jako Administrator Danych Osobowych Liceum Ogólnokształcącego im. Stefana Żeromskiego w Bartoszycach upoważniam do przetwarzania danych osobowych:

Upoważniam Pana/Panią* .....

do przetwarzania danych osobowych w zakresie następujących procesów:

- *prowadzenie bieżącej rekrutacji,*
- *wykorzystywanie dokumentów aplikacyjnych kandydatów do pracy w przyszłych rekrutacjach,*
- *realizacja praw i obowiązków pracowniczych w ramach zatrudnienia,*
- *przetwarzanie danych w ramach Zakładowego Funduszu Świadczeń Socjalnych,*
- *wykorzystywanie wizerunku pracowników,*
- *podnoszenie kwalifikacji i szkolenia pracowników*
- *ewidencja korespondencji oraz odbiór i wysyłanie korespondencji,*
- *księgowanie i archiwizowanie dokumentów,*
- *prowadzenie rekrutacji uczniów,*
- *wykorzystywania wizerunku uczniów potrzebnego do realizowania obowiązków statutowych szkoły,*
- *przekazywanie danych niezbędnych do prowadzenia polityki edukacyjnej szkoły i państwa,*
- *edukacji uczniów.*
- *wychowawczego,*
- *opiekuńczego.*

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 Administratora Danych Osobowych)

*niepotrzebne skreślić

ZAŁĄCZNIK NR 2B. WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH (SEKRETARIAT)

Bartoszyce, dnia .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

UPOWAŻNIENIE nr ..... z dn. .....
obowiązuje od .....

Na podstawie art. 29 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO,** jako Administrator Danych Osobowych Liceum Ogólnokształcącego im. Stefana Żeromskiego w Bartoszycach upoważniam do przetwarzania danych osobowych:
Upoważniam Pana/Panią* .....
do przetwarzania danych osobowych w zakresie następujących procesów:

- *prowadzenie bieżącej rekrutacji,*
- *wykorzystywanie dokumentów aplikacyjnych kandydatów do pracy w przyszłych rekrutacjach,*
- *realizacja praw i obowiązków pracowniczych w ramach zatrudnienia,*
- *przetwarzanie danych w ramach Zakładowego Funduszu Świadczeń Socjalnych,*
- *wykorzystywanie wizerunku pracowników,*
- *podnoszenie kwalifikacji i szkolenia pracowników*
- *ewidencja korespondencji oraz odbiór i wysyłanie korespondencji,*
- *księgowanie i archiwizowanie dokumentów,*
- *prowadzenie rekrutacji uczniów,*
- *wykorzystywania wizerunku uczniów potrzebnego do realizowania obowiązków statutowych szkoły,*
- *przekazywanie danych niezbędnych do prowadzenia polityki edukacyjnej szkoły i państwa,*
- *edukacji uczniów.*

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 Administratora Danych Osobowych)

*niepotrzebne skreślić

ZAŁĄCZNIK NR 2C. WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH (NAUCZYCIELE)

Bartoszyce, dnia .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

UPOWAŻNIENIE nr ..... z dn. .....
obowiązuje od .....

Na podstawie art. 29 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO,** jako Administrator Danych Osobowych Liceum Ogólnokształcącego im. Stefana Żeromskiego w Bartoszycach upoważniam do przetwarzania danych osobowych:

Upoważniam Pana/Panią* .....
do przetwarzania danych osobowych w zakresie następujących procesów:

- *rekrutacji uczniów,*
- *edukacyjnego,*
- *wychowawczego,*
- *opiekuńczego,*

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 Administratora Danych Osobowych)

*niepotrzebne skreślić

ZAŁĄCZNIK NR 2D. WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH (FŚS)

Bartoszyce, dnia .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

UPOWAŻNIENIE nr ..... z dn. .....
obowiązuje od .....

Na podstawie art. 29 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO** oraz z powodu prac w Komisji Świadczeń Socjalnych jako Administrator Danych Osobowych Liceum Ogólnokształcącego im. Stefana Żeromskiego w Bartoszycach upoważniam do przetwarzania danych osobowych:

Upoważniam Pana/Panią* .....
do przetwarzania danych osobowych w zakresie następujących procesów:

- *przetwarzanie danych w ramach Zakładowego Funduszu Świadczeń Socjalnych,*

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 Administratora Danych Osobowych)

*niepotrzebne skreślić

ZAŁĄCZNIK NR 3. WZÓR EWIDENCJI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W LICEUM OGÓLNOKSZTAŁCĄCYM IM. STEFANA ŻEROMSKIEGO

Lp	Imię i nazwisko	Stanowisko / komórka organizacyjna	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Identyfikator w danym systemie

ZAŁĄCZNIK NR 4. WZÓR ODWOŁANIA UPOWAŻNIENIA DO PRZETWARZANIA DANYCH

Bartoszyce, dnia .....

ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem ..... na podstawie art. 29 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO ,** jako Administrator Danych Osobowych Liceum Ogólnokształcącego im. Stefana Żeromskiego w Bartoszycach **odwołuję**

upoważnienie nr ..... Pana/Pani* .....
do przetwarzania danych osobowych w zakresie następujących procesów:

- prowadzenie bieżącej rekrutacji,
- wykorzystywanie dokumentów aplikacyjnych kandydatów do pracy w przyszłych rekrutacjach,
- realizacja praw i obowiązków pracowniczych w ramach zatrudnienia,
- przetwarzanie danych w ramach Zakładowego Funduszu Świadczeń Socjalnych,
- wykorzystywanie wizerunku pracowników,
- podnoszenie kwalifikacji i szkolenia pracowników
- ewidencja korespondencji oraz odbiór i wysyłanie korespondencji,
- księgowanie i archiwizowanie dokumentów,
- prowadzenie rekrutacji uczniów,
- wykorzystywania wizerunku uczniów potrzebnego do realizowania obowiązków statutowych szkoły,
- przekazywanie danych niezbędnych do prowadzenia polityki edukacyjnej szkoły i państwa,
- edukacji uczniów.
- wychowawczego,
*- opiekuńczego.**

.....
(podpis Administratora Danych Osobowych)

*niepotrzebne skreślić

ZAŁĄCZNIK NR 5. WZÓR OŚWIADCZENIA O ZAPOZNANIU SIĘ Z DOKUMENTACJĄ, JEJ ZROZUMIENIEM ORAZ ZACHOWANIEM POUFNOŚCI.

Bartoszyce, ...

OŚWIADCZENIE

Stwierdzam własnoręcznym podpisem, że znana mi jest treść „Dokumentacji ochrony danych osobowych" Liceum Ogólnokształcącego im. Stefana Żeromskiego w Bartoszycach oraz zostałem zapoznany z **Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) i Ustawie o Ochronie Danych Osobowych z 10 maja 2018 r.**

Jednocześnie zobowiązuję się do:

* stosowania określonych przez Administratora Danych Osobowych zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne w stosunku do celu przetwarzanie danych,
* należytego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym,
* zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony osób, których dane dotyczą,
* zachowania w tajemnicy danych oraz ich sposobu zabezpieczeń, nawet po ustaniu stosunku pracy.

W zakresie systemu informatycznego zobowiązuję się:

* nie ujawniać danych zawartych w eksploatowanych systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
* nie ujawniać szczegółów technologicznych w używanych systemach oraz oprogramowaniu,
* nie udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
* nie kopiować i nie przetwarzać danych w sposób inny niż dopuszczony obowiązującą Dokumentacją.

Zobowiązuję się do:

- zachowania w tajemnicy **danych osobowych,** do których mam lub będę miał/a dostęp w trakcie wykonywania czynności zleconych przez Pracodawcę w fizycznym obszarze przetwarzania, których Administratorem Danych Osobowych jest Liceum Ogólnokształcące im. Stefana Żeromskiego w Bartoszycach
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych bezpośredniemu przełożonemu.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższym zobowiązaniem, może być uznane za naruszenie przepisów karnych Ustawy o ochronie danych osobowych.

(podpis pracownika) (podpis dyrektora)

ZAŁĄCZNIK NR 6. WZÓR OŚWIADCZENIA O ZACHOWANIU POUFNOŚCI PRZEZ PRACOWNIKÓW OBSŁUGI

Bartoszyce, ...

OŚWIADCZENIE

Zobowiązuję się do:

- zachowania w tajemnicy **danych osobowych,** których Administratorem jest Liceum Ogólnokształcące im. Stefana Żeromskiego w Bartoszycach
  i do których mam lub będę miał/a dostęp w trakcie wykonywania czynności zleconych przez Pracodawcę w fizycznym obszarze przetwarzania,
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych bezpośredniemu przełożonemu.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższym zobowiązaniem, może być uznane za naruszenie przepisów karnych Ustawy o ochronie danych osobowych.

(podpis pracownika) (podpis dyrektora)

ZAŁĄCZNIK NR 7. WZÓR RAPORTU Z PRZEPROWADZONEJ KONTROLI PRZEZ INSPEKTORA DANYCH OSOBOWYCH

RAPORT Z KONTOLI BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

W LICEUM OGÓLNOSZTAŁCĄCYM im. STEFANA ŻEROMSKIEGO

W BARTOSZYCACH

1. Data przeprowadzenia kontroli: .....

2. Naruszenia ochrony danych osobowych:

LP	czas, miejsce,	osoby powiadamiające, zaangażowane lub odpytywane	okoliczności towarzyszące naruszeniu i rodzaj naruszenia	opis podjętego działania	ocena przyczyn naruszenia	ocena przeprowadzonego postępowania wyjaśniającego i naprawczego

.....

(podpis Administrator danych)

.....

(podpis inspektora ochrony danych)

ZAŁĄCZNIK NR 8. ZGODA RODZICA NA WYKORZYSTANIE DANYCH OSOBOWYCH /WIZERUNKU DZIECKA W CELU PROMOWANIA SZKOŁY I INFORMOWANIU O JEJ DZIAŁALNOŚCI

.....

(miejscowość, data)

Ja, niżej podpisany(a), ... wyrażam zgodę na
(imię i nazwisko rodzica/prawnego opiekuna)

przetwarzanie danych osobowych mojego dziecka ..... przez
(imię i nazwisko ucznia)

Liceum Ogólnokształcące im. Stefana Żeromskiego w Bartoszycach oraz dodatkowo wyrażam zgodę:*

	TAK	**NIE**
- na wykorzystanie danych w celu promowania szkoły i informowaniu o jej działalności (sukcesy w konkursach, świadectwa z wyróżnieniem, projekty, uroczystości itp.)		
- na wykorzystanie wizerunku (sukcesy w konkursach, świadectwa z wyróżnieniem, projekty, uroczystości itp.)		

*** Zgoda całkowicie dobrowolna. Niewyrażenie jej nie skutkuje żadnymi konsekwencjami.**

Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady z dnia 27 kwie tnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu informacji takich danych w UE (RODO) informuję, że:

1) Administratorem danych osobowych jest Liceum Ogólnokształcące im. Stefana Żeromskiego w Bartoszycach ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce. Szkoła gromadzi i przetwarza dane osobowe na podstawie i w granicach przepisów prawa, w szczególności prawa oświatowego i kodeksu pracy w celu realizacji zdań statutowych.
2) Inspektorem Ochrony Danych jest osoba wyznaczona przez Administratora Danych Osobowych, e-mail: lo@bartoszyce.info, nr tel. (89) 762 28 59.
3) Dane osobowe nie są udostępniane innym odbiorcom oprócz podmiotów upoważnionych na podstawie przepisów prawa.
4) Administrator nie przekazuje danych osobowych do państwa trzeciego ani do organizacji międzynarodowych.
5) Dane osobowe będą przetwarzane nie dłużej niż jest to konieczne, tj. przez okres wyznaczony właściwym przepisem prawa.
6) Każdej osobie przysługuje prawo dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania oraz prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed cofnięciem.
7) W związku z przetwarzaniem danych osobowych przez Administratora istnieje prawo wniesienia skargi do organu nadzorczego, który zajmuje się ochroną danych osobowych. W Polsce jest to Prezes Urzędu Ochrony Danych Osobowych (PUODO), który zastąpił Generalnego Inspektora Ochrony Danych Osobowych (GIODO), ul. Stawki 2, 00-193 Warszawa.
8) Dane osobowe są przetwarzane w formie papierowej i elektronicznej.
9) Dane osobowe nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.

.....

(podpis rodzica/prawnego opiekuna)

ZAŁĄCZNIK NR 9. ZGODA PEŁNOLETNIEGO UCZNIA NA WYKORZYSTANIE DANYCH OSOBOWYCH/WIZERUNKU W CELU PROMOWANIA SZKOŁY I INFORMOWANIU O JEJ DZIAŁALNOŚCI.

.....
(miejscowość, data)

Ja, niżej podpisany(a), ... wyrażam zgodę na
(imię i nazwisko)

przetwarzanie moich danych osobowych przez Liceum Ogólnokształcące im. Stefana Żeromskiego

w Bartoszycach oraz dodatkowo wyrażam zgodę:*

	TAK	**NIE**
- na wykorzystanie danych w celu promowania szkoły i informowaniu o jej działalności (sukcesy w konkursach, świadectwa z wyróżnieniem, projekty, uroczystości itp.)		
- na wykorzystanie wizerunku (sukcesy w konkursach, świadectwa z wyróżnieniem, projekty, uroczystości itp.)		

*** Zgoda całkowicie dobrowolna. Niewyrażenie jej nie skutkuje żadnymi konsekwencjami.**

Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady z dnia 27 kwie tnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu informacji takich danych w UE (RODO) informuję, że:

1) Administratorem danych osobowych jest Liceum Ogólnokształcące im. Stefana Żeromskiego w Bartoszycach ul. Bohaterów Monte Cassino 9 11-200 Bartoszyce. Szkoła gromadzi i przetwarza dane osobowe na podstawie i w granicach przepisów prawa, w szczególności prawa oświatowego i kodeksu pracy w celu realizacji zdań statutowych.
2) Inspektorem Ochrony Danych jest osoba wyznaczona przez Administratora Danych Osobowych, e-mail: lo@bartoszyce.info, nr tel. (89) 762 28 59.
3) Dane osobowe nie są udostępniane innym odbiorcom oprócz podmiotów upoważnionych na podstawie przepisów prawa.
4) Administrator nie przekazuje danych osobowych do państwa trzeciego ani do organizacji międzynarodowych.
5) Dane osobowe będą przetwarzane nie dłużej niż jest to konieczne, tj. przez okres wyznaczony właściwym przepisem prawa.
6) Każdej osobie przysługuje prawo dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania oraz prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed cofnięciem.
7) W związku z przetwarzaniem danych osobowych przez Administratora istnieje prawo wniesienia skargi do organu nadzorczego, który zajmuje się ochroną danych osobowych. W Polsce jest to Prezes Urzędu Ochrony Danych Osobowych (PUODO), który zastąpił Generalnego Inspektora Ochrony Danych Osobowych (GIODO), ul. Stawki 2, 00-193 Warszawa.
8) Dane osobowe są przetwarzane w formie papierowej i elektronicznej.
9) Dane osobowe nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.

.....
(podpis ucznia)

ZAŁĄCZNIK NR 10. ZGODA RODZICA/UCZNIA NA WYKORZYSTANIE DANYCH OSOBOWYCH/WIZERUNKU W CELU UCZESTNICZENIA W ZAWODACH / KONKURSACH / OLIMPIADACH

.....
(miejscowość, data)

Ja, niżej podpisany(a), ... wyrażam zgodę na
(imię i nazwisko rodzica/prawnego opiekuna)

uczestniczenie mojego syna /córki* .....

w .....
(nazwa zawodów, konkursu, olimpiady oraz nazwa organizatora)

*** niepotrzebne skreślić**

Jednocześnie wyrażam zgodę na wykorzystanie danych osobowych oraz wizerunku w celach określonych regulaminem imprezy. Oświadczam, że u mojego dziecka nie występują problemy zdrowotne uniemożliwiające mu uczestniczenie w wyżej wymienionej imprezie i wyrażam zgodę na wykonanie niezbędnych zabiegów medycznych ratujących życie i zdrowie mojego dziecka.

....
(podpis rodzica/prawnego opiekuna) *(podpis ucznia)*

ZAŁĄCZNIK NR 11. LISTA OSÓB, KTÓRE ZAPOZNAŁY SIĘ Z DOKUMENTACJĄ OCHRONY DANYCH LICEUM OGÓLNOKSZTAŁCĄCEGO IM. STEFANA ŻEROMSKIEGO W BARTOSZYCACH

L.p.	Imię i nazwisko	Data	Podpis
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			

26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			
36.			
37.			
38.			
39.			
40.			
41.			
42.			
43.			
44.			
45.			