POLITYKA BEZPIECZEŃSTWA

MONIKA FRANCZUK-FRYSZ ANGIELSKI
ZAKĄTEK SZKOŁA JĘZYKA ANGIELSKIEGO
44-240 ŻORY
Ul. Rybnicka 92

Spis treści

I. WSTĘP

1 DEKLARACJE

1) Monika Franczuk-Frysz prowadząca działalność gospodarczą pod firmą Angielski Zakątek Szkoła Języka Angielskiego Monika Franczuk-Frysz świadoma wagi zagrożeń jakie niesie ze sobą przetwarzanie danych osobowych dla wolności i praw osób, których dane dotyczą, uznaje zapewnienie bezpieczeństwa tych danych jako jeden z priorytetów swojej działalności.
2) W celu realizacji zadania określonego w pkt. 1 ustanawia się Politykę Bezpieczeństwa danych osobowych oraz Instrukcję Zarządzania Systemem Informatycznym.
3) Dokumenty opisane w pkt 2) stanowią łącznie dokumentację przetwarzania danych osobowych w firmie Angielski Zakątek Szkoła Języka Angielskiego Monika Franczuk-Frysz.
4) Polityka Bezpieczeństwa określa organizację i infrastrukturę przetwarzania danych osobowych jak również wskazuje szczegółowe działania, jakie należy podjąć oraz ustanawia reguły postępowania, których należy przestrzegać, aby właściwie realizować obowiązki z zakresu ochrony danych osobowych.
5) Wszystkie osoby dopuszczone do przetwarzania danych osobowych w firmie Angielski Zakątek Szkoła Języka Angielskiego Monika Franczuk-Frysz są zobowiązane do stosowania zasad i procedur ustanowionych w celu zapewnienia ochrony przetwarzanych danych osobowych, zarówno tych zawartych w Polityce Bezpieczeństwa jak i w innych dokumentach stworzonych w tym zakresie.
6) Firma Angielski Zakątek Szkoła Języka Angielskiego Monika Franczuk-Frysz deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania takim zagrożeniom jak:
   a) sytuacje losowe lub nieprzewidziane działanie czynników zewnętrznych np. pożar, zalanie pomieszczeń, kradzież, włamanie, napad, niepożądana ingerencja osób trzecich,
   b) niewłaściwe parametry środowiska pracy urządzeń komputerowych (nadmierna wilgotność, nadmierna temperatura),
   c) awarie sprzętu lub oprogramowania wskazujące na naruszenie ochrony danych osobowych, niewłaściwe działanie serwisantów w tym pozostawienie bez nadzoru lub poza siedzibą administratora danych,
   d) naruszenie bezpieczeństwa przez nieautoryzowane ich przetwarzanie, ujawnienie osobom nieupoważnionym procedur ochrony stosowanych przez administratora,
   e) ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora, w tym także nieumyślne ujawnienie danych (praca bez upoważnienia, naruszanie polityki ochrony haseł),
   f) celowe lub przypadkowe rozproszenie danych w sieci publicznej,
   g) ataki z sieci publicznej,
   h) naruszenie zasad i procedur określonych w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznymi.
7) Wszelkie wątpliwości dotyczące sposobu interpretacji postanowień dokumentów wchodzących w skład dokumentacji przetwarzania danych osobowych powinny być rozstrzygane ze szczególnym uwzględnieniem ochrony danych osobowych osób fizycznych na adekwatnym do zagrożeń poziomie bezpieczeństwa.

2 ZAKRES STOSOWANIA

1) Zasady i procedury określone w dokumentach wchodzących w skład dokumentacji przetwarzania danych osobowych stosuje się zarówno do danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach, listach i innych zbiorach ewidencyjnych, jak również i w systemach informatycznych.
2) Zasady i procedury, o których mowa powyżej stosuje się do wszystkich osób przetwarzających dane osobowe w firmie Angielski Zakątek Szkoła Języka Angielskiego Monika Franczuk-Frysz, zarówno do osób bezpośrednio zatrudnionych w strukturach organizacyjnych, jak i osób świadczących pracę na podstawie umów cywilno-prawnych.

3 OPIS DOKUMENTU

1) Niniejsza Polityka Bezpieczeństwa danych osobowych określa sposób przetwarzania danych osobowych przez firmę Angielski Zakątek Szkoła Języka Angielskiego Monika Franczuk-Frysz jako Administratora Danych Osobowych.
2) Polityka Bezpieczeństwa zawiera w szczególności:
   a) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
   b) rejestr czynności przetwarzania, w tym dla poszczególnych czynności przetwarzania:
      - cele przetwarzania;
      - opis kategorii osób, których dane dotyczą, oraz kategorii przetwarzanych danych osobowych;
      - kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
      - planowane terminu usunięcie poszczególnych kategorii danych;
   c) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa – zapewniających stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych, których dane dotyczą
3) Ponadto, w Polityce Bezpieczeństwa określone zostały środki techniczne i organizacyjne niezbędne dla zapewnienia rozliczalności przetwarzanych danych osobowych, tj. przestrzegania następujących zasad:
   a) zgodności z prawem, rzetelności i przejrzystości;
   b) ograniczonego celu;
   c) minimalizacji danych;
   d) prawidłowość danych;
   e) ograniczonego przechowywania; oraz
   f) integralności i poufności danych.
4) Dodatkowo integralną częścią niniejszej Polityki Bezpieczeństwa jest „Ocena obowiązku wyznaczenia Inspektora Ochrony Danych”, na podstawie której Administrator Danych Osobowych podjął decyzje o braku konieczności wyznaczenia Inspektora Ochrony Danych.

II. POSTANOWIENIA OGÓLNE

1 DEFINICJA POJĘĆ ZASTOSOWANYCH W NINIEJSZEJ POLITYCE BEZPIECZEŃSTWA

Ilekroć w niniejszej Polityce jest mowa o:

1) **Ustawie** – rozumie się przez to ustawę o ochronie danych osobowych z dnia 10 maja 2018 roku;
2) **Rozporządzeniu Unijnym, Rozporządzeniu, RODO** – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy Unii Europejskiej nr L 119/1 z 04 kwietnia 2016 roku);
3) **Polityce Bezpieczeństwa, Polityce** – rozumie się przez to niniejszy dokument stanowiący integralną cześć dokumentacji przetwarzania danych osobowych u Administratora Danych Osobowych;
4) **Instrukcji Zarządzania Systemem Informatycznym, Instrukcji** – rozumie się przez to dokument stanowiący integralną część dokumentacji przetwarzania danych osobowych w systemach informatycznych Administratora Danych Osobowych;
5) **Administratorze Danych Osobowych, Administratorze Danych, ADO** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W rozumieniu niniejszej Polityki Bezpieczeństwa Administratorem Danych Osobowych jest Monika Franczuk-Frysz prowadząca działalność gospodarczą pod firmą Angielski Zakątek Szkoła Języka Angielskiego Monika Franczuk-Frysz z siedzibą w Żorach, Os. Pawlikowskiego PU12;
6) **Danych Osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą").
7) **Możliwej do zidentyfikowania osobie fizycznej** – rozumie się przez to osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
8) **Szczególnych kategoriach danych osobowych, danych wrażliwych** – rozumie się dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osób fizycznych lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tych osób;
9) **Danych biometrycznych** – rozumie się przez to 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;
10) **Zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
11) **Przetwarzaniu danych** – 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;

12) **Pełnomocniku Ochrony Danych, POD** – rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, odpowiedzialną za zapewnianie, aby przetwarzanie danych osobowych przez Administratora Danych Osobowych odbywało się zgodnie z przepisami o ochronie danych osobowych. Szczegółowy zakres obowiązków POD określa niniejsza Polityka. Pełnomocnik Ochrony Danych nie jest Inspektorem Ochrony Danych, o którym mowa w art. 37-39 RODO, w związku z czym ADO nie ma obowiązku publikacji danych kontaktowych Pełnomocnika Ochrony Danych i zawiadomienia o nich Organu Nadzorczego.
13) **Sieci Informatycznej** – rozumie się przez to zespół połączonych, współpracujących ze sobą urządzeń, programów, narzędzi informatycznych i systemów informatycznych używanych u Administratora Danych Osobowych;
14) **Systemie informatycznym** - rozumie się przez to program komputerowy, służący do przetwarzania danych osobowych, do którego dostęp wymaga uwierzytelniania za pośrednictwem identyfikatora i hasła;
15) **Osobie upoważnionej do przetwarzania danych osobowych** - rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych;
16) **Użytkowniku** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych w systemach informatycznych, której nadano identyfikator i przyznano hasło;
17) **Podmiocie Przetwarzającym** – rozumie się przez osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych;
18) **Odbiorcy** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców;
19) **Identyfikatorze** – rozumie się przez to ciąg znaków literowych, cyfrowych i innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
20) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych i innych znany jedynie osobie uprawnionej do pracy w systemie informatycznym, tj. Użytkownikowi;
21) **Sieci publicznej** - rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt. 29 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne (Dz.U.2017.1907 t.j. z dnia 2017.10.12);
22) **Naruszeniu ochrony danych osobowych** - rozumie się przez to 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;
23) **Organie Nadzorczym** – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych;
24) **Profilowaniu** – rozumie się przez to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

25) **Pseudonimizacji** - rozumie się przez to 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;
26) **usłudze społeczeństwa informacyjnego** – rozumie się przez to usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (1), tj. usługę świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług;

2 CEL STOSOWANIA I PODSTAWY PRAWNE

1) Wdrożenie Polityki Bezpieczeństwa u Administratora Danych ma na celu zabezpieczenie przetwarzanych u niego danych osobowych, w tym bezpieczeństwa danych przetwarzanych w systemach informatycznych i poza nimi oraz zapewnienie zgodności działania Administratora Danych z RODO i Ustawą.
2) Dokument Polityki Bezpieczeństwa został opracowany na podstawie przepisów zawartych w poniższych aktach:
   a) Rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy Unii Europejskiej nr L 119/1 z 04 kwietnia 2016 roku);
   b) Ustawie z dnia 10 maja 2018 roku o ochronie danych osobowych;
   c) Ustawie z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz.U.2018.108 t.j. z dnia 2018.01.12);
   d) Ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2017.1219 t.j. z dnia 2017.06.24);
   e) Ustawie z dnia 16 lipca 2004 r. prawo telekomunikacyjne (Dz.U.2017.1907 t.j. z dnia 2017.10.12);
3) Niniejszy dokument wraz z dokumentami powiązanymi opisuje niezbędny do uzyskania zbiór warunków technicznych i organizacyjnych, jakim powinny odpowiadać wszelkie czynności przetwarzania danych osobowych jak również urządzenia i systemy informatyczne służące do ich przetwarzania.

III. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

1 ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH [ADO]

1) Administrator Danych Osobowych podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem zmian w obowiązującym prawie, działalności gospodarczej prowadzonej przez Administratora Danych Osobowych oraz technik zabezpieczania danych osobowych.
2) Administrator Danych Osobowych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:
   a) pseudonimizację i szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

3) Oceniając, czy stopień bezpieczeństwa jest odpowiedni, Administrator Danych Osobowych uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w tym wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
4) Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, Administrator Danych Osobowych, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, wdraża odpowiednie środki techniczne i organizacyjne (takie jak np. pseudonimizacja) zaprojektowane w celu skutecznej realizacji zasad ochrony danych (takich jak np. minimalizacja danych) oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą („privacy by design”).
5) Administrator Danych Osobowych wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane, bez interwencji danej osoby, nieokreślonej liczbie osób fizycznych („privacy by default”).
6) Administrator Danych Osobowych podejmuje działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia Administratora Danych Osobowych, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie Administratora Danych Osobowych.
7) Administrator Danych Osobowych realizuje zadania w zakresie ochrony danych osobowych, a w szczególności zapewnia to, by dane osobowe były:
   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
   b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”);
   c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
   d) prawidłowe i w razie potrzeby uaktualniane („prawidłowość”);
   e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”);
   f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz

przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

8) Administrator Danych Osobowych jest odpowiedzialny za wypełnianie zasad określonych w pkt 7) powyżej i powinien wykazać ich przestrzeganie („rozliczalność").
9) Administrator Danych Osobowych realizuje swoje obowiązki osobiście bądź za pośrednictwem upoważnionych do tego osób, w tym zwłaszcza Pełnomocnika Ochrony Danych.
10) Administrator Danych Osobowych upoważnia poszczególne osoby do przetwarzania danych osobowych w stosownym, indywidualnie określonym zakresie.
11) Administrator Danych Osobowych może wyznaczyć Pełnomocnika Ochrony Danych oraz określić zakres jego zadań i czynności.
12) Administrator Danych Osobowych zapewnia możliwość zapoznania się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
13) Administrator Danych Osobowych zapewnia użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne i zgodne z prawem przetwarzanie danych.
14) Administrator Danych Osobowych podejmuje działania w przypadku stwierdzenia naruszenia ochrony danych osobowych, w tym działania określone w art. 33 i art. 34 RODO.

2 ZADANIA PEŁNOMOCNIKA OCHRONY DANYCH [POD]

1) Administrator Danych Osobowych może powołać Pełnomocnika Ochrony Danych, którego zadaniem ma być zapewnienie wykonywania przez Administratora Danych Osobowych obowiązków wynikających z obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz niniejszej Polityki Bezpieczeństwa.
2) Pełnomocnik Ochrony Danych zobowiązany jest również do bieżącego śledzenia zmian w przepisach obowiązującego prawa (z zakresu danych osobowych) oraz informowania ADO o zmianach i treści tych zmian.
3) W przypadku niepowołania Pełnomocnika Ochrony Danych, zadania wskazane w niniejszym pkt [zadania pełnomocnika ochrony danych] wykonuje Administrator Danych Osobowych.
4) W celu zapewnienia wykonywania przez ADO obowiązków z zakresu ochrony danych osobowych Pełnomocnik Ochrony Danych realizuje bieżący nadzór nad przestrzeganiem zasad ochrony danych osobowych, a w szczególności:
   a) sprawuje nadzór nad wdrożeniem środków organizacyjnych, technicznych i fizycznych celem zapewnienia bezpieczeństwa danych osobowych;
   b) kontroluje obieg i sposób przechowywania dokumentów zawierających dane osobowe;
   c) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń oraz prowadzeniem wszelkich ewidencji z zakresu ochrony danych osobowych;
   d) prowadzi dokumentację dotyczącą ochrony danych osobowych;
   e) zawiera umowy powierzenia przetwarzania danych osobowych, w sytuacjach, w których jest to niezbędne;
   f) nadzoruje udostępnianie danych osobowych odbiorcom i innym podmiotom;
   g) prowadzi, nadzoruje i aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych;
   h) nadzoruje i zatwierdza nowe procesy biznesowe, i informatyczne, i zmiany w istniejących w zakresie prawidłowości przetwarzania danych osobowych;

i) nadzoruje realizację obowiązku zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie tych danych, w szczególności decyduje o terminach i sposobach przeprowadzania szkoleń w tym zakresie;
j) zatwierdza wzory dokumentów i zgód (odpowiednie klauzule w dokumentach) dotyczących ochrony danych osobowych;
k) prowadzi ewidencję osób upoważnionych do przetwarzania;

5) Pełnomocnik Ochrony Danych reprezentuje Administratora Danych Osobowych w kontaktach z Organem Nadzorczym, w tym zwłaszcza dokonuje zgłoszeń naruszeń jak również reprezentuje ADO w trakcie przeprowadzanych przez Organ Nadzorczy kontroli.
6) Pełnomocnik Ochrony Danych reprezentuje ADO w kontaktach z osobami, których dane dotyczą, w tym pełni nadzór nad przesyłaniem im stosowanych informacji, oraz udzielaniem im odpowiedzi na kierowane do ADO żądania, zwłaszcza związane z przysługującymi osobom fizycznym na mocy RODO prawami (art. 15-22 RODO).
7) Pełnomocnik Ochrony Danych udziela zaleceń co do oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych oraz monitoruje wykonanie tychże oceny.
8) Ponadto Pełnomocnik Ochrony Danych dba o systemy informatyczne, w których przetwarzane są dane osobowe w szczególności poprzez
   a) zarządzanie systemami informatycznymi i aplikacjami przetwarzającymi dane osobowe, w tym:
      - wykonywanie i odpowiednie przechowywanie kopii zapasowych,
      - zabezpieczanie systemów i aplikacji przed działaniem złośliwego oprogramowania,
      - zabezpieczanie systemów i aplikacji przed wszelkimi zagrożeniami pochodzącymi z sieci publicznej.
   b) przeciwdziałanie dostępowi osób niepowołanych do systemów informatycznych i aplikacji;
   c) prowadzenie dokumentacji i raportowanie Pełnomocnikowi Ochrony Danych wszelkich naruszeń bezpieczeństwa systemów informatycznych i aplikacji;
   d) odpowiadanie za poprawne działanie systemów informatycznych, nadzorowanie wykonywanie napraw, prac konserwacyjnych komputerów i innych urządzeń mających wpływ na bezpieczeństwo danych osobowych;
   e) przydzielanie identyfikatorów i haseł do systemów informatycznych i aplikacji oraz ich modyfikację, w tym wyrejestrowywanie użytkowników;
   f) nadzorowanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do systemów informatycznych i aplikacji;
   g) podejmowanie działań służących zapewnieniu niezawodności zasilania komputerów i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
9) W innych sprawach związanych z przetwarzaniem danych osobowych, a w szczególności naruszeń współdziała z ADO;
10) Pełnomocnik Ochrony Danych, w celu wykonywania wskazanych powyżej zadań, uprawniony jest do:
    a) uzyskiwania wszelkich informacji dotyczących przetwarzania danych osobowych, od wszystkich komórek organizacyjnych ADO,

b) kontrolowania funkcjonowania systemu zabezpieczeń zarówno fizycznych jak informatycznych
c) uzyskiwania wyjaśnień i pomocy od wszystkich pracowników ADO w sytuacjach naruszenia bezpieczeństwa danych osobowych lub w związku z nieprawidłowościami lub zagrożeniami związanymi z ochroną danych osobowych.

11) Zadania Pełnomocnika Ochrony Danych wykonuje osoba wyznaczona w tym celu przez Administratora Danych Osobowych.

3 OBOWIĄZKI OSOBY UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH OSOBOWYCH

1) Każda osoba działająca z upoważnienia Administratora i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie Administratora.
2) Osoba upoważniona do przetwarzania danych może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych lub Pełnomocnika Ochrony Danych (o ile został powołany) i tylko w celu wykonywania swoich obowiązków.
3) Zakres dostępu do danych osobowych przetwarzanych w danym systemie informatycznym przypisany jest do niepowtarzalnego identyfikatora Użytkownika, którego podanie niezbędne jest do rozpoczęcia pracy w systemie informatycznym.
4) Rozwiązanie stosunku służbowego powoduje wygaśnięcie upoważnienia do przetwarzania danych.
5) Każdy osoba upoważniona do przetwarzania danych osobowych zobowiązuje się pisemnie do zachowania w tajemnicy, przez cały okres zatrudnienia u Administratora Danych Osobowych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji, danych osobowych.
6) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do przestrzegania obowiązujących u Administratora Danych Osobowych zasad i procedur bezpieczeństwa przetwarzania danych osobowych. Naruszenie zasad i procedur bezpieczeństwa, a w szczególności udostępnienie danych osobie niepowołanej jest naruszeniem obowiązków służbowych.
7) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do:
   a) zapoznania się z przepisami prawa w zakresie ochrony danych, z przepisami niniejszej Polityki oraz Instrukcji Zarządzania Systemami Informatycznymi;
   b) stosowania się do procedur i wytycznych oraz poleceń służbowych wydawanych przez Administratora Danych Osobowych oraz Pełnomocnika Ochrony Danych (o ile został powołany) mających na celu zgodne z prawem przetwarzanie danych;
   c) zabezpieczenia danych przed ich udostępnianiem osobom nieupoważnionym;
   d) korzystania z systemów informatycznych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników.

IV. OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH

Adres	Kondygnacja i nr pokoju lub pomieszczenia	Nazwa pomieszczenia	Określenie czynności przetwarzania	Funkcja pomieszczenia	Szczególne zabezpieczenia pomieszczenia, inne uwagi
Ul. Rybnicka 92	Parter	Pomieszczenie biurowe	Wszystkie czynności	Wszelkie czynności, w tym modyfikowanie,	

44-240 Żory			wskazane w załączniku PB-Z2a	przeglądanie, wprowadzanie, usuwanie, udostępnianie itp.	

Administrator Danych Osobowych przetwarza dane osobowe w następujących lokalizacjach:

V. WYKAZ SYSTEMÓW INFORMATYCZNYCH, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

nazwa i opis	zastosowania systemu
System informatyczny GSuite for Education	System obsługujący platformę edukacyjną
System informatyczny Microsoft Office 365	Głównie w czynnościach doraźnych, w tym ewidencja kursantów, wystawianie certyfikatów, bieżąca korespondencji, tworzenie umów
System Ing.ksiegowosc.pl	Wystawianie rachunków i faktur

VI. REJESTR CZYNNOŚCI PRZETWARZANIA

1) Rejestr czynności przetwarzania zawarty jest w załącznikach:
   a) Załączniku nr PB-Z2a – Rejestr czynności przetwarzania danych osobowych – administrator danych.
   b) Załączniku nr PB-Z2b – Rejestr czynności przetwarzania danych osobowych – podmiot przetwarzający.

VII. EWIDENCJE

1) Administrator Danych Osobowych prowadzi następujące ewidencje wchodzące w skład dokumentacji ochrony danych osobowych:
   a) ewidencję osób upoważnionych do przetwarzania danych osobowych;
   b) ewidencję udostępnień danych osobowych odbiorcom oraz innym podmiotom. Każdorazowe udostępnienie danych osobowych ze zbiorów danych przetwarzanych przez Administratora wymaga podania podstawy prawnej;
   c) ewidencję komputerów i urządzeń przenośnych;
   d) ewidencję naruszeń.

VIII. POSTANOWIENIA KOŃCOWE

1) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych osobowych z niniejszą Polityką oraz Instrukcją Zarządzania Systemami Informatycznymi.

2) Naruszenie zasad i procedur określonych w niniejszy dokumencie może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.
3) W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy RODO, a także przepisy Ustawy oraz inne powszechnie obowiązujące przepisy prawa.
4) Administrator Danych Osobowych, może zmieniać niniejszą Politykę Bezpieczeństwa.

IX. WYKAZ ZAŁĄCZNIKÓW

1) Załączniki stanowią integralną część Polityki Bezpieczeństwa:
   a) Załącznik nr PB-Z1: Ocena obowiązku wyznaczenia Inspektora Ochrony Danych
   b) Załącznik nr PB-Z2a: Rejestr czynności przetwarzania – administrator danych
   c) Załącznik nr PB-Z2b: Rejestr czynności przetwarzania - podmiot przetwarzający
   d) Załącznik nr PB-Z3: ogólny opis technicznych i organizacyjnych środków bezpieczeństwa niezbędnych dla zapewnienia rozliczalności przetwarzanych danych osobowych.
   e) Załącznik nr PB-Z4a: Wzory dokumentów.
   f) Załącznik nr PB-Z4b: Wzory rejestrów
   g) Załącznik nr PB-Z5: Założenia i schematy procedur dotyczących praw osób fizycznych art. 15-22 RODO