Polityka bezpieczeństwa przetwarzania danych osobowych
w Stowarzyszeniu Nauczycieli Języka Angielskiego w Polsce IATEFL Poland
(International Association of Teachers of English as a Foreign Language in Poland, IATEFL POLAND)

Rozdział 1
Postanowienia ogólne

§ 1

Celem Polityki bezpieczeństwa przetwarzania danych osobowych, zwanej dalej „Polityką bezpieczeństwa" w Stowarzyszeniu Nauczycieli Języka Angielskiego w Polsce IATEFL Poland, zwanym dalej „Stowarzyszeniem", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2

Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:

- Rozporządzeniu Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.1/,
- Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych /opracowana na podstawie Dz. U. z 2018 r., poz. 1000, 1669/.

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

§ 4

Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Stowarzyszeniu rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
2. integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3. rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
4. integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;

5. dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
6. zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 5

Administratorem danych osobowych jest Stowarzyszenie Nauczycieli Języka Angielskiego w Polsce IATEFL Poland, International Association of Teachers of English as a Foreign Language in Poland IATEFL POLAND z siedzibą w Zgorzelcu pod adresem: Armii Krajowej 51A, 59-900 Zgorzelec, REGON: 350324970.

§ 6

Polityka bezpieczeństwa ma zastosowanie do wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

Rozdział 2
Definicje

§ 7

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1. **administrator danych osobowych –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
2. **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych /opracowana na podstawie Dz. U. z 2018 r., poz. 1000, 1669/.
3. **RODO** – rozporządzenie Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str. 1/,
4. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
5. **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
6. **przetwarzanie danych –** operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.,

7. **system informatyczny –** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
8. **system tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
9. **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
10. **administrator systemu informatycznego** – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,
11. **odbiorca –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
12. **strona trzecia –** osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,
13. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
14. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3
Zakres stosowania

§ 8

1. W Stowarzyszeniu Nauczycieli Języka Angielskiego w Polsce IATEFL Poland przetwarzane są dane osobowe członków zebrane w zbiorach danych osobowych.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
4. Innymi dokumentami regulującymi ochronę danych osobowych w Stowarzyszeniu są:
   a) ewidencja osób upoważnionych do przetwarzania danych osobowych,
   b) procedura postępowania w przypadku naruszenia ochrony danych osobowych

§ 9

Politykę bezpieczeństwa stosuje się w szczególności do:

1. danych osobowych przetwarzanych w systemie: *Microsoft Office, Conference Management System - system pocztowy, Płatnik, system bankowości elektronicznej, system do kontaktu z US, RAKS, Linuxpl, wordpress.*

2. wszystkich informacji dotyczących danych członków,
3. odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia,
4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób trzecich mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych,
6. innych dokumentów zawierających dane osobowe.

§ 10

1. Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:

   a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
   b) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   c) wszystkich pracowników i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty zobowiązani są wszyscy członkowie, osoby współpracujące oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

Rozdział 4
Wykaz zbiorów danych osobowych

§ 11

1. Wykaz zbiorów, w których gromadzone są dane osobowe wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi:

Nr	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
1.	**Kontrahenci**	System pocztowy System bankowości	Dane osobowe są przetwarzane w celu wystawienia faktury, rachunku lub prowadzenia	Dane osobowe kontrahentów, zleceniobiorców, wolontariuszy przetwarzane	imię, nazwisko, adres zamieszkania, NIP, numer telefonu, adres e-mail, numer rachunku bankowego, imię (imiona) i nazwisko, nazwisko rodowe, imię matki i ojca, data i miejsce urodzenia, obywatelstwo, PESEL, miejsce zameldowania, zamieszkania, korespondencji (kod pocztowy, miejscowość, ulica, nr domu i	

		elektronicznej System do kontaktu z Urzędem Skarbowym Contro RAKS Płatnik	sprawozdawczości finansowej, kontaktu, dokonania zgłoszeń do Urzędu Skarbowego, ZUS.	w związku z realizacją zawartych umów oraz świadczeniem usług, jak również realizowaniem obowiązków wynikających z przepisów prawa w związku z zawartymi umowami.	lokalu, gmina, powiat, województwo), telefon, US, NFZ, prawo do emerytury/renty, st. niepełnosprawności, wykształcenie (nazwa szkoły, zawód, specjalność, stopień naukowy i zawodowy, wykształcenie uzupełniające , osiągnięty przychód, informacja o prowadzeniu działalności gospodarczej	
2.	**Członkowie Stowarzyszenia**	System pocztowy Contro	Dane osobowe przetwarzane w związku z prowadzeniem działalności Stowarzyszenia.	Dane osobowe członków Stowarzyszenia.	imię, nazwisko, adres, adres e-mail, numer telefonu, przedział wiekowy, zawód, kwalifikacje, długość doświadczenia zawodowego	
3.	**Uczestnicy Konferencji**	Conference Management System System pocztowy	Dane osobowe przetwarzane w celu organizacji Konferencji.	Dane osobowe uczestników konferencji oraz prelegentów.	imię, nazwisko, numer telefonu, adres e-mail, adres do korespondencji, miejsce zatrudnienia, opis kwalifikacji/doświadczenia	
4.	**Uczestnicy Konkursów**	System pocztowy	Dane osobowe przetwarzane w celu organizacji konkursu, t.j. m.in. identyfikacji uczestników oraz wydania nagród.	Dane osobowe uczestników konkursu.	imię, nazwisko, data urodzenia, nazwa szkoły, klasa oraz imię i nazwisko nauczyciela	
5.	**Odbiorcy Newslettera**	System pocztowy	Dane osobowe osób korzystających z Newslettera	Dane osób korzystających z Newslettera.	imię, nazwisko, adres e-mail, nazwa firmy (miejsce zatrudnienia)	

		Contro	przetwarzane w celu wysyłki Newslettera.			

Rozdział 5
Sposób przepływu danych osobowych pomiędzy systemami informatycznymi

§ 12

Dane z systemu Conference Management System są jednostronnie eksportowane do systemu pocztowego służącego do wysłania mailingu.

Dane osobowe z systemu wordpress nie są eksportowane do innego systemu oraz nie są importowane. Osoba, której dane dotyczą samodzielnie wprowadza dane do systemu poprzez stronę internetową www.

Rozdział 6
Wykaz budynków, pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych

§ 13

Dane osobowe przetwarzane są w budynku, mieszczącym się w Zgorzelcu przy Armii Krajowej 51A.

Rozdział 7
Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§ 14

Środki ochrony fizycznej danych osobowych

Środek ochrony fizycznej danych	Uwagi
Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).	Tak
Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.	Tak
Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.	Tak
Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.	Tak
Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.	Tak

§ 15

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

Środek sprzętowy infrastruktury informatycznej i telekomunikacyjnej	Uwagi
Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.	Tak
Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.	Tak
Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.	Nie dotyczy, gdyż dane są przetwarzane na laptopach.

Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	Tak, laptopy posiadają odrębne konta użytkowników, których identyfikacja odbywa się za pomocą 8 znakowego hasła (małe i wielkie litery ,cyfry, znaki specjalne).
Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.	Tak, dyski komputerów są szyfrowane.
Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.	Brak systemu wymuszającego zmianę hasła, lecz osoby upoważnione są zobowiązane do zmiany hasła co 30 dni, o czym są systematycznie powiadamiane drogą mailową.
Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.	Tak
Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.	Tak, wysyłane pliki z danymi są szyfrowane
Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.	Tak

Użyto system Firewall do ochrony dostępu do sieci komputerowej.	Tak

§ 16

Środki ochrony w ramach narzędzi programowych i baz danych

Środki ochrony w ramach narzędzi programowych i baz danych	Uwagi
Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.	Tak
Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.	Tak
Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	Tak, hasło składa się z 8 znaków (małe i wielkie litery, cyfry, znaki specjalne).
Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.	Tak
Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.	Brak systemu wymuszającego zmianę hasła, lecz osoby upoważnione są zobowiązane do zmiany hasła co 30 dni

Zastosowano kryptograficzne środki ochrony danych osobowych.	Tak
Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.	Tak
Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.	Tak

§ 17

Środki organizacyjne

Środek organizacyjny	Uwagi
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.	Tak
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.	Tak
Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy.	Tak
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.	Tak
Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.	Tak

Rozdział 8
Zadania administratora danych osobowych

§ 18

Do najważniejszych obowiązków administratora danych osobowych należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa i innymi dokumentami wewnętrznymi,
3. przeprowadzenie oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych – w przypadku, gdy organizacja wprowadza nowy rodzaj przetwarzania danych osobowych,
4. stworzenie procedur postępowania w sytuacjach naruszenia ochrony danych osobowych,
5. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
6. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
7. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
8. nadzór nad bezpieczeństwem danych osobowych,
9. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
10. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Rozdział 9
Postanowienia końcowe

§ 19

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych.
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.

5. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki bezpieczeństwa, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Załączniki:

1. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych
2. Ocena ryzyka
3. Upoważnienie do przetwarzania danych osobowych - wzór
4. Zgoda na przetwarzanie danych osobowych - wzór
5. Zgoda na wykorzystanie wizerunku – wzór

Data aktualizacji: 29.06.2022