Polityka bezpieczeństwa przetwarzania danych osobowych

SPEAKOUT
szkoła językowa

Speak Out Sp. z o.o.
Ul. Lutosławskiego 6
27-200 Starachowice
NIP 6642151471

Data sporządzenia: 5 kwietnia 2018 r.

SPIS TREŚCI

ROZDZIAŁ 1.	DEFINICJE	3
ROZDZIAŁ 2.	POSTANOWIENIA OGÓLNE	5
ROZDZIAŁ 3.	ADMINISTRATOR I OSOBY UPOWAŻNIONE	6
	ADMINISTRATOR	6
	OSOBY UPOWAŻNIONE	6
ROZDZIAŁ 4.	ZBIORY I PRZECHOWYWANIE DANYCH OSOBOWYCH	7
	DANE OSOBOWE UCZNIÓW I OPIEKUNÓW PRAWNYCH	7
	DANE OSOBOWE PRACOWNIKÓW	8
	ZBIORY DANYCH OSOBOWYCH	9
	PRZECHOWYWANIE DANYCH OSOBOWYCH	10
ROZDZIAŁ 5.	BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH	11
	ZABEZPIECZENIE NOŚNIKÓW DANYCH I POMIESZCZEŃ	11
	ZABEZPIECZENIE KOMPUTERÓW	12
	ZABEZPIECZENIE NOŚNIKÓW DANYCH	14
	ŚRODKI ORGANIZACYJNE	14
ROZDZIAŁ 6.	UPRAWNIENIA OSÓB, KTÓRYCH DOTYCZĄ DANE OSOBOWE	15
ROZDZIAŁ 7.	POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH	16
ROZDZIAŁ 8.	RYZYKO NARUSZENIA OCHRONY DANYCH OSOBOWYCH	16
ROZDZIAŁ 9.	PROCEDURA W PRZYPADKU NARUSZENIA OCHRONY DANYCH	17
ROZDZIAŁ 10.	POSTANOWIENIA KOŃCOWE	17
ROZDZIAŁ 11.	ZAŁĄCZNIKI	18

ROZDZIAŁ 1. DEFINICJE

Terminy użyte w niniejszej Polityce Bezpieczeństwa przetwarzania danych osobowych mają następujące znaczenie:

1) **„Administrator"** oznacza

Speak Out Sp. z o.o. ul. Lutosławskiego 6, 27-200 Starachowice NIP 664 215 14 71 wpisany do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Kielc Wydział X Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0001024508

2) **„dane osobowe"** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą");

3) **„Komputer"** oznacza komputer stacjonarny, laptop lub tablet;

4) **„Kurs Językowy"** oznacza zajęcia dla Uczniów i Uczniów Pełnoletnich w Szkole, w ramach których Administrator prowadzi nauczanie języka obcego;

5) **„Lektor"** oznacza osobę prowadzącą Kurs Językowy, niezależnie od podstawy prawnej łączącej go z Administratorem;

6) **„Lokal Szkoły"** oznacza miejsce, w którym mogą być przechowywane i przetwarzane są dane osobowe;

7) „**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;

8) **„Nośniki Cyfrowe"** oznaczają płyty CD, DVD, karty pamięci, dyski twarde (w tym dyski przenośne), pendrive'y, pamięci flash i inne urządzenia, na których przechowywane są dane osobowe w formacie cyfrowym;

9) **„Nośniki Fizyczne"** oznaczają wydruki, formularze, umowy i inne materiały mające postać papierową, na których przechowywane są dane osobowe;

10) **„Osoba Upoważniona"** oznacza Pracownika mającego dostęp do danych osobowych i przetwarzającego je na polecenie Administratora;

11) **„Opiekun Prawny"** oznacza opiekuna prawnego, który zawarł lub zamierza zawrzeć umowę z Administratorem o prowadzenie Kursu Językowego na rzecz Ucznia;

12) **„Podmiot Przetwarzający”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

13) **„Polityka Bezpieczeństwa”** oznacza niniejszą politykę bezpieczeństwa przetwarzania danych osobowych;

14) **„Pracownik”** oznacza osobę wykonującą na rzecz Administratora pracę bądź świadczącą na jego rzecz usługi niezależnie od podstawy prawnej łączącej go z Administratorem, w tym Lektora;

15) **„przetwarzanie”** 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;

16) **„RODO”** oznacza 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);

17) **„Sekretariat”** oznacza miejsce w Lokalu Szkoły, do którego dostęp mają Uczniowie, Uczniowie Pełnoletni, Opiekunowie Prawni i osoby trzecie, a w którym przebywa Pracownik Administratora odpowiedzialny za bieżącą obsługę administracyjną i organizacyjną Szkoły;

18) **„Szkoła”** oznacza szkołę językową, w ramach której Administrator prowadzi kursy językowe;

19) **„Uczeń”** oznacza osobę małoletnią, która bierze udział w Kursie Językowym prowadzonym przez Administratora w ramach Szkoły;

20) **„Uczeń Pełnoletni”** oznacza osobę pełnoletnią, która bierze udział w Kursie Językowym prowadzonym przez Administratora w ramach Szkoły;

21) **„Umowa dotycząca Kursu Językowego”** oznacza umowę dotyczącą możliwości uczestnictwa w Kursie Językowym zawartą pomiędzy Administratorem a Opiekunem Prawnym albo Administratorem a Uczniem Pełnoletnim;

22) **„ustawa o ochronie danych osobowych”/„uodo”** oznacza ustawę o ochronie danych osobowych;

23) **„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;

24) **„zgoda”** 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.

ROZDZIAŁ 2. POSTANOWIENIA OGÓLNE

2.1. Polityka Bezpieczeństwa jest dokumentem, który określa zasady przetwarzania danych osobowych oraz wdrożone w Szkole środki techniczne i organizacyjne mające zapewnić, by przetwarzanie danych osobowych następowało w sposób gwarantujący odpowiednie bezpieczeństwo i poufność, w tym ochronę przed:

1) niedozwolonym lub niezgodnym z prawem przetwarzaniem;
2) utratą, zniszczeniem lub uszkodzeniem danych osobowych;
3) nieuprawnionym dostępem do danych osobowych i sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych osobowych i z tego sprzętu.

2.2. Celem przyjęcia Polityki Bezpieczeństwa jest wykazanie, że Administrator przestrzega przepisów RODO.

2.3. Polityka Bezpieczeństwa znajduje zastosowanie do danych osobowych przetwarzanych w Szkole w sposób zautomatyzowany oraz w sposób ręczny, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych.

2.4. Polityka Bezpieczeństwa obowiązuje wszystkich Pracowników Administratora oraz inne osoby, o ile Administrator zobowiązał je do przestrzegania postanowień Polityki Bezpieczeństwa.

2.5. Dane osobowe przetwarzane są w systemie informatycznym oraz fizycznych zbiorach danych, przechowywanych w Lokalu Szkoły znajdującym się przy ul. Ul. Spółdzielcza 33, 27-200 Starachowice i ul. Witolda Lutosławskiego 6,27-200 Starachowice.

2.6. Dane osobowe Uczniów, Uczniów Pełnoletnich, Opiekunów Prawnych i Pracowników mogą być udostępniane Teddy Eddie sp. z o.o., ul. Jasna 31B, 44-100 Gliwice oraz podmiotom współpracującym z tą spółką, a także innym podmiotom, stosownie do zgód udzielonych przez Opiekunów Prawnych, Uczniów Pełnoletnich oraz Pracowników. Administrator może powierzyć przetwarzanie danych osobowych w oparciu o umowę o powierzeniu przetwarzania danych osobowych.

2.9 Polityka Bezpieczeństwa została opracowana zgodnie z wymogami 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).

ROZDZIAŁ 3. ADMINISTRATOR I OSOBY UPOWAŻNIONE

Administrator

3.1 Administratorem danych osobowych przetwarzanych w Szkole jest

Speak Out Sp. z o.o. ul. Lutosławskiego 6, 27-200 Starachowice NIP 664 215 14 71 wpisany do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Kielc Wydział X Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0001024508

3.2 Administrator zapewnia, że Polityka Bezpieczeństwa jest przestrzegana i że dane osobowe są:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie są dalej przetwarzane w sposób niezgodny z tymi celami;
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, dla których są przetwarzane;
4) prawidłowe i w razie potrzeby uaktualniane;
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres wskazany w Polityce Bezpieczeństwa;
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem

przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą środków technicznych i organizacyjnych, o których mowa w Polityce Bezpieczeństwa.

3.3 Realizując powyższe postanowienia Administrator podejmuje wszelkie niezbędnie działania w celu ochrony danych osobowych, a w szczególności:

1) stosuje procedury i środki techniczne oraz organizacyjne opisane w Polityce Bezpieczeństwa;
2) prowadzi dokumentację potwierdzającą prawidłowość przetwarzania danych osobowych;
3) wyznacza Osoby Upoważnione do przetwarzania danych osobowych;
4) zapoznaje Osoby Upoważnione z treścią Polityki Bezpieczeństwa;
5) nadzoruje i kontroluje przestrzeganie Polityki Bezpieczeństwa i przepisów RODO oraz uodo przez Osoby Upoważnione;
6) zapewnia, że osoby których dane dotyczą, mogą korzystać z praw przyznanych im przez przepisy prawa.

Osoby Upoważnione

3.4 Administrator nadaje upoważnienia do przetwarzania danych osobowych każdej osobie, która ma dostęp do danych osobowych przetwarzanych w Szkole. Osobami Upoważnionymi mogą być w szczególności Pracownicy oraz osoby odpowiedzialne za zabezpieczenie systemów informatycznych używanych w Szkole, jeśli nie są Pracownikami.

3.5 Osoba, której nadano upoważnienie uzyskuje status Osoby Upoważnionej i może przetwarzać dane osobowe w Szkole.

3.6 Nadanie upoważnienia następuje w formie pisemnej przez złożenie oświadczenia przez Administratora. Oświadczenie składane jest na formularzu stanowiącym załącznik nr 2 do Polityki Bezpieczeństwa i dotyczy konkretnej osoby.

3.7 Administrator prowadzi ewidencję Osób Upoważnionych. Ewidencja wskazuje imiona i nazwiska Osób Upoważnionych oraz datę nadania upoważnienia. Wzór ewidencji stanowi załącznik nr 3 do Polityki Bezpieczeństwa.

3.8 Osoby Upoważnione zostają zapoznane z treścią Polityki Bezpieczeństwa i zobowiązane do przestrzegania jej postanowień.

3.9 Każda Osoba Upoważniona zobowiązana jest do przetwarzania danych osobowych zgodnie z RODO, uodo i Polityką Bezpieczeństwa, a w szczególności do:

1) ochrony danych osobowych przetwarzanych w Szkole Administratora;
2) zachowania w tajemnicy treści Polityki Bezpieczeństwa, w szczególności w zakresie środków technicznych i organizacyjnych stosowanych przez Administratora w celu ochrony danych osobowych;
3) niezwłocznego informowania Administratora o zauważonych naruszeniach lub podejrzeniach naruszenia środków technicznych i organizacyjnych stosowanych przez Administratora w celu ochrony danych osobowych;
4) zachowania w tajemnicy danych osobowych, do których ma dostęp, również po ustaniu stosunku prawnego łączącego ją z Administratorem;
5) nie wynoszenia na jakichkolwiek nośnikach danych osobowych z Lokalu Szkoły, chyba że Administrator wyraził na to zgodę;
6) przestrzegania środków technicznych i organizacyjnych opisanych w Polityce Bezpieczeństwa.

ROZDZIAŁ 4. ZBIORY I PRZECHOWYWANIE DANYCH OSOBOWYCH

Dane osobowe Uczniów, Uczniów Pełnoletnich i Opiekunów Prawnych

4.1. Administrator przetwarza dane osobowe Uczniów, Uczniów Pełnoletnich i Opiekunów Prawnych.

4.2. Dane osobowe Opiekuna Prawnego i Ucznia są podawane przez Opiekuna Prawnego w związku z wolą zawarcia z Administratorem Umowy dotyczącej Kursu Językowego. Dane osobowe Ucznia Pełnoletniego podawane są przez niego w związku z wolą zawarcia z Administratorem Umowy dotyczącej Kursu Językowego. Dane osobowe mogą być podane na Formularzu Zgłoszeniowym stanowiącym załącznik nr 1 do Polityki Bezpieczeństwa lub w inny sposób – tj. na przykład przez podanie ich na listach osób zainteresowanych.

4.3. Dane osobowe Uczniów, Uczniów Pełnoletnich i Opiekunów Prawnych są przetwarzane m.in. w następujących celach:

1) zawarcia i prawidłowej realizacji umowy dotyczącej prowadzenia kursu językowego;
2) marketingu bezpośredniego Administratora.

4.4. Administrator zbiera wyłącznie takie dane osobowe Opiekunów Prawnych, Uczniów i Uczniów Pełnoletnich, które są niezbędne dla celów, dla których są przetwarzane.

4.5. Administrator może zbierać dane osobowe dotyczące zdrowia Ucznia, jeżeli Opiekun prawny przekazał Administratorowi informacje dotyczące problemów zdrowotnych, które mogą mieć znaczenie dla uczestnictwa w Kursie. Dane dotyczące zdrowia mogą w szczególności dotyczyć rodzaju produktów, na które Uczeń jest uczulony.

4.6. Podstawą przetwarzania danych osobowych Ucznia, Ucznia Pełnoletniego i Opiekuna Prawnego są: (i) zgoda (ii) niezbędność przetwarzania danych do wykonania Umowy dotyczącej Kursu Językowego, (iii) prawnie uzasadniony interes realizowany przez Administratora tj. marketing bezpośredni.

4.7. Formularz Zgłoszeniowy zawiera treść zgód na przetwarzanie danych osobowych wyrażanych przez Opiekuna Prawnego lub Ucznia Pełnoletniego.

4.8. Wzory zgód na przetwarzanie danych osobowych i na korzystanie z wizerunku wyrażone przez Opiekuna Prawnego lub Ucznia Pełnoletniego stanowią załącznik nr 5 do Polityki Bezpieczeństwa.

Dane osobowe Pracowników

4.9. Administrator przetwarza dane osobowe Pracowników.

4.10. Dane osobowe Pracowników są przetwarzane przez Administratora w związku ze świadczeniem przez nich pracy, usług lub dostaw na rzecz Administratora.

4.11. Dane osobowe Pracownika są przetwarzane w celach:
1) zawarcia i realizacji Umowy łączącej go z Administratorem;
2) zapewnienia Pracownikowi dostępu do internetowych funkcjonalności będących częścią kursów językowych takich jak np. Teddy Eddie.

4.12. Administrator zbiera wyłącznie takie dane osobowe Pracowników, które są niezbędne dla celów, dla których są przetwarzane.

4.13. Podstawą przetwarzania danych osobowych Pracownika jest niezbędność przetwarzania danych w celu wykonywania umowy łączącej go z Administratorem.

4.14. W zakresie w jakim dane osobowe Pracownika przetwarzane są w celu zapewnienia Pracownikowi dostępu do internetowych funkcjonalności będących częścią kursu językowego (takich jak np. Teddy Eddie), podstawą

przetwarzania danych osobowych jest zgoda Pracownika. Zgoda ta dotyczy wprowadzenia danych osobowych do serwisu internetowego (np. www.bs.edubears.pl) oraz udostępnienia tych danych podmiotowi zarządzającemu serwisem (np. Teddy Eddie sp. z o. o).

4.15. Pracownik może również wyrazić zgody dotyczące korzystania z jego wizerunku, w tym:
1) zgodę na rejestrowanie na nagraniach audiowizualnych wizerunku Pracownika w trakcie prowadzenia zajęć językowych oraz na udostępnienie przez Szkołę nagrań zawierających powyższy wizerunek spółce Teddy Eddie sp. z o. o. z siedzibą w Gliwicach (44-100) przy ul. Jasnej 31b oraz podmiotom współpracującym z tą spółką;
2) zgodę na rejestrowanie na nagraniach audiowizualnych i fotografiach jego wizerunku, w trakcie eventów organizowanych przez Szkołę oraz na udostępnianie tych nagrań i fotografii w celach marketingowych i informacyjnych związanych z działalnością Administratora.

4.16. Administrator może również przetwarzać dane osobowe kandydatów na Pracowników, którzy wyrazili wolę uczestnictwa w procesie rekrutacyjnym i przesłali informację zawierającą ich dane osobowe. Dane osobowe kandydatów na Pracowników przetwarzane są w celu prowadzenia procesów rekrutacyjnych.

Zbiory danych osobowych

4.18. Administrator przechowuje dane osobowe w zbiorach. Zbiory mogą mieć formę elektroniczną lub papierową.

4.19. Odrębne zbiory obejmują dane osobowe Uczniów, Uczniów Pełnoletnich i Opiekunów Prawnych. W zbiorach tych określa się następujące informacje:
1) dane osobowe Ucznia i Opiekuna Prawnego oraz Ucznia Pełnoletniego podane na Formularzu Zgłoszeniowym i Umowie dotyczącej Kursu Językowego;
2) datę zawarcia Umowy dotyczącej Kursu Językowego;
3) rodzaje zgód na przetwarzanie danych osobowych, które zostały wyrażone przez Opiekuna Prawnego i datę wyrażenia poszczególnych zgód.

4.20. Dane osobowe Pracowników są przetwarzane w odrębnych zbiorach. Zbiory te mogą obejmować również dane osób będących kandydatami na Pracowników. W zbiorach określa się następujące informacje:

1) dane osobowe Pracownika podane przez niego Administratorowi;
2) datę zawarcia umowy łączącej Pracownika z Administratorem;
3) rodzaje zgód na przetwarzanie danych osobowych, które zostały wyrażone przez Pracownika i datę wyrażenia poszczególnych zgód.

4.21. Administrator może stworzyć odrębne zbiory obejmujące dane osobowe Opiekunów Prawnych i Uczniów Pełnoletnich, które są przetwarzane w celach marketingowych. W zbiorach tych określa się następujące informacje:
1) imię i nazwisko;
2) numer telefonu;
3) adres e-mail.

Przechowywanie danych osobowych

4.22. Dane osobowe mogą być przetwarzane wyłącznie w określonych obszarach tj. na terenie Lokalu Szkoły lub na terenie budynku, gdzie odbywają się zajęcia, (jeśli nie odbywają się one na terenie Lokalu Szkoły). Postanowienie to nie dotyczy przetwarzania danych osobowych w systemach informatycznych, które mogą być przetwarzane na Komputerach poza w/w obszarami.

4.23. Dane osobowe podane przez Opiekuna Prawnego/Ucznia Pełnoletniego przechowywane są w wersjach papierowych na Nośnikach Fizycznych. Dane osobowe podane przez Opiekuna Prawnego/Ucznia Pełnoletniego wprowadzane i przechowywane są:

- Na nośnika papierowych
- Na dysku internetowym zabezpieczonym hasłem

4.24. Dane osobowe podane przez Pracownika przechowywane są w wersjach papierowych na Nośnikach Fizycznych. Dane osobowe podane przez Pracownika wprowadzane są również do plików zapisanych w systemie informatycznym na Komputerze.

4.25. Dane osobowe podane przez Opiekunów Prawnych/Uczniów Pełnoletnich i Pracowników mogą być przechowywane i przetwarzane w ramach korzystania przez Administratora z informatycznych usług cloud computingu (tzw. „chmury") dostarczanych przez podmioty trzecie. Przetwarzanie w ramach chmury może dotyczyć w szczególności poczty elektronicznej oraz tzw. wirtualnych dysków. Administrator będzie korzystał z usług cloud computingu dostarczanych wyłącznie przez zaufane podmioty dające gwarancje przestrzegania przepisów RODO.

4.26. Dane osobowe znajdujące się na Nośnikach Fizycznych przechowywane są na terenie Lokalu Szkoły lub na terenie budynku, gdzie odbywają się zajęcia, jeśli nie odbywają się one na terenie Lokalu Szkoły.

4.27. Dane osobowe znajdujące się na Nośnikach Fizycznych Administrator może zdigitalizować i przechowywać wyłącznie w formie cyfrowej. W takim przypadku Nośniki Fizyczne Administrator może zniszczyć za pomocą niszczarki dokumentów gwarantującej zachowanie poziomu bezpieczeństwa.

4.28. Dane osobowe Uczniów, Uczniów Pełnoletnich Opiekunów Prawnych i Pracowników przechowywane są przez okres 10 lat liczonych od dnia wygaśnięcia stosunku prawnego łączącego danego Opiekuna Prawnego lub Pracownika z Administratorem. Po upływie tego okresu dane osobowe są usuwane ze zbiorów.

ROZDZIAŁ 5. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

5.1. W celu zapewnienia bezpieczeństwa przetwarzanych danych osobowych Administrator wdraża opisane poniżej środki techniczne i organizacyjne. W razie potrzeby środki bezpieczeństwa będą poddawane przeglądom i zostaną uaktualnione.

5.2. Wdrożone środki techniczne i organizacyjne odpowiadają charakterowi, zakresowi, kontekstowi i celom przetwarzania oraz ryzyku naruszenia praw lub wolności osób, których dane są przetwarzane.

5.3. Obowiązki Administratora, o których mowa niżej dotyczą również Osób Upoważnionych.

5.4. Administrator prowadzi rejestr czynności przetwarzania danych osobowych w związku z tym, że przetwarza dane osobowe dotyczące zdrowia Uczniów. Wzór rejestru czynności stanowi załącznik nr 6.

Zabezpieczenie nośników danych i pomieszczeń

5.5. Lokal Szkoły zabezpieczony jest przed nieuprawnionym dostępem osób trzecich przez zamknięcie drzwi wejściowych na klucz poza godzinami pracy Szkoły i włączeniem alarmu.

5.6. Administrator zabezpiecza przed nieuprawnionym dostępem osób trzecich pomieszczenia, w których może znajdować się dokumentacja zawierająca dane osobowe – Nośniki Fizyczne i Nośniki Cyfrowe.

5.7. Nośniki Fizyczne i Nośniki Cyfrowe, które nie są aktualnie wykorzystywane przez Administratora lub Osoby Upoważnione, są przechowywane przez Administratora w szafie zamykanej na klucz, w miejscu niedostępnym dla osób trzecich.

5.8. Zarówno pomieszczenia jak i szafa, w której przechowywane są Nośniki Fizyczne i Nośniki Cyfrowe powinny być każdorazowo zamykane na klucz. Klucze do drzwi i szaf powinny być przechowywane w wyznaczonym przez Administratora miejscu i nie mogą zostać pozostawione w zamkach. Dostęp do kluczy mają jedynie Administrator oraz Osoby Upoważnione.

5.9. Osoby Upoważnione przestrzegają tzw. „zasady czystego biurka", która oznacza, że nie można pozostawiać dokumentacji związanej z danymi osobowymi, w tym Nośników Fizycznych lub Nośników Cyfrowe, w sposób, który mógłby umożliwić zapoznanie się przez osoby trzecie z treścią danych osobowych. Za realizację „zasady czystego biurka" odpowiedzialna jest każda Osoba Upoważniona oraz Administrator – w zakresie swoich stanowisk pracy.

5.10. Nośniki Fizyczne, które stały się zbędne, niezwłocznie należy zniszczyć za pomocą niszczarki dokumentów gwarantującej zachowanie poziomu bezpieczeństwa. Nośniki Cyfrowe, które stały się zbędne, niezwłocznie należy zniszczyć w sposób uniemożliwiający zapoznanie się z danymi albo usunąć trwale znajdujące się na nich dane osobowe.

5.11. Administrator stosuje dodatkowe środki zabezpieczenia pomieszczeń takie jak:
1) alarm;
2) monitoring;
3) ochrona budynku;

5.12. Jeżeli Szkoła dysponuje Sekretariatem, Administrator dba o zabezpieczenie Sekretariatu adekwatne do przetwarzanych danych osobowych.

5.13. W przypadku korzystania w Sekretariacie z komputera bądź innego urządzenia wyposażonego w monitor, monitor powinien być ustawiony w sposób uniemożliwiający osobom trzecim wgląd do danych wyświetlanych na monitorze.

5.14. W przypadku konieczności opuszczenia przez Osobę Upoważnioną stanowiska komputerowego w Sekretariacie, Komputer powinien zostać zablokowany w sposób uniemożliwiający dostęp do niego osobom trzecim.

5.15. W Sekretariacie nie można pozostawiać Nośników Fizycznych i Nośników Danych w sposób umożliwiający dokonanie ich kradzieży lub przypadkowego zabrania przez osoby trzecie.

5.16. W przypadku, gdyby w Sekretariacie znajdował się firmowy telefon komórkowy lub inne urządzenie elektroniczne, na którym znajdowałyby się dane osobowe, telefon (urządzenie) zostanie zabezpieczony przez ustawienie kodu wymaganego do odblokowania ekranu telefonu. W przypadku gdyby Osoba Upoważniona przetwarzała dane osobowe na prywatnym telefonie komórkowym lub innym urządzeniu elektronicznym, jest ona zobowiązana do zabezpieczenia telefonu (urządzenia) w sposób opisany w zdaniu pierwszym.

Zabezpieczenie Komputerów

5.17. Komputery, na których przetwarzane są dane osobowe w Szkole są podłączone do sieci internet.

5.18. Dane osobowe mogą być przetwarzane na Komputerach będących własnością Administratora lub – za zgodą Administratora – na Komputerze będącym własnością Osoby Upoważnionej, o ile zabezpieczy ona taki Komputer zgodnie z poniższymi postanowieniami. W takim przypadku Pracownik jest zobowiązany przestrzegać postanowień dotyczących zabezpieczania Komputera również w trakcie użytkowania Komputera w czasie, w którym nie świadczy pracy lub usług na rzecz Administratora.

5.19. Dostęp do Komputera, na którym przetwarzane są dane osobowe zabezpieczony jest przez wymóg podania indywidualnego loginu i hasła przypisanego konkretnej Osobie Upoważnionej. Tego rodzaju zabezpieczanie zobowiązana jest stosować również Osoba Upoważniona, która przetwarza dane osobowe na Komputerze będącym jej własnością.

5.20. Osoby Upoważnione zobowiązane są do przechowywania loginów i haseł w bezpiecznym miejscu i nieudostępniania ich innym. Osoby Upoważnione nie są uprawnione do zmiany hasła na Komputerze będącym własnością Administratora bez zgody Administratora.

5.21. Po zakończonej pracy lub w przypadku opuszczania stanowiska pracy Osoba Upoważniona powinna wylogować się ze swojego konta.

5.22. W przypadku korzystania z usług cloud computingu (tzw. „chmury") dostarczanych przez podmioty trzecie, dostęp do takiej usługi zabezpieczony jest loginem i hasłem. Osoby Upoważnione zobowiązane są do przechowywania loginów i haseł w bezpiecznym miejscu i nieudostępniania ich innym. Osoby Upoważnione nie są uprawnione do zmiany hasła.

5.23. Dostęp do internetowej platformy do zarządzania szkołą językową, plików przechowywanych na Komputerze i kont umożliwiających korzystanie z usług cloud computingu mają jedynie Administrator i Osoby Upoważnione.

5.24. Spis loginów i haseł do wszystkich usług cloud computingu oraz spis loginów i haseł przypisanych poszczególnym Osobom Upoważnionym przechowywany będzie przez Administratora w miejscu, niedostępnym ani dla Osób Upoważnionych, ani dla osób trzecich.

5.25. Hasła używane przez Administratora oraz Osoby Upoważnione posiadają co najmniej 5 znaków (w przypadku telefonów i tabletów dopuszczalne jest hasło zawierające 4 znaki).

5.26. Administrator stosuje szyfrowanie danych oraz szyfrowanie wiadomości e-mail przesyłanych za pośrednictwem poczty elektronicznej.

5.27. Każdy Komputer, na którym przetwarzane są dane osobowe jest wyposażony w program antywirusowy, którego celem będzie wykrywanie, zwalczanie i usuwanie wirusów komputerowych. Program antywirusowy powinien gwarantować zachowanie poziomu bezpieczeństwa adekwatnego do przetwarzanych danych. W ustawieniach programu antywirusowego włączona powinna być opcja aktualizacji automatycznych.

5.28. Osoby Upoważnione mogą pobierać na Komputerze pliki z internetu jednie z zaufanych źródeł. W przypadku pobrania pliku z niezaufanego źródła powinien on zostać niezwłocznie usunięty – bez otwierania.

5.29. System operacyjny każdego Komputera, na którym przetwarzane są dane osobowe, powinien być aktualizowany niezwłocznie po ukazaniu się kolejnych oficjalnych aktualizacji.

5.30. Administrator raz na dwa miesiące wykonuje kopie zapasowe danych osobowych przetwarzanych w Szkole. Wykonane kopie zapasowe zapisywane są na nośniku przechowywanym w zabezpieczonym miejscu.

Zabezpieczenie Nośników Danych

5.31. Osoby Upoważnione mogą przy przetwarzaniu danych osobowych korzystać z Nośników Danych.

5.32. Każda z Osób Upoważnionych powinna zabezpieczyć Nośnik Danych przed jego zniszczeniem, kradzieżą lub przypadkową utratą.

5.33. Każdy Nośnik Cyfrowy powinien być zabezpieczony hasłem lub szyfrowaniem w celu uniemożliwienia osobom nieupoważnionym uzyskania dostępu do znajdujących się na nim danych. Osoby Upoważnione nie są uprawnione do zmiany hasła bez zgody Administratora.

5.34. Nośniki Cyfrowe, które uległy uszkodzeniu można przekazać do naprawy pod warunkiem uzyskania od podmiotu, który ma dokonać naprawy zobowiązania do zachowania w poufności danych osobowych znajdujących się na Nośniku Cyfrowym.

5.35. Osoba Upoważniona niezwłocznie zawiadomi Administratora o utracie Nośnika Cyfrowego i wskaże dane osobowe, które znajdowały się na Nośniku Cyfrowym.

Środki organizacyjne

5.36. Administrator zapoznaje Osoby Upoważnione z treścią Polityki Bezpieczeństwa i przepisami RODO oraz uodo.

5.37. Administrator kontroluje przestrzeganie Polityki Bezpieczeństwa i przepisów RODO oraz uodo przez Osoby Upoważnione.

5.38. Niedopuszczalne jest wynoszenie jakichkolwiek materiałów zawierających dane osobowe poza Lokal Szkoły lub miejsce, w którym odbywają się zajęcia, chyba że Administrator wyrazi na to zgodę. Postanowienie to nie dotyczy Komputerów i telefonów, na których przetwarzane są dane osobowe w Szkole, a które są własnością Osób Upoważnionych.

ROZDZIAŁ 6. UPRAWNIENIA OSÓB, KTÓRYCH DOTYCZĄ DANE OSOBOWE

6.1. Administrator zapewnia osobom, których dane dotyczą możliwość korzystania z wszelkich uprawnień przyznanych im przez RODO i uodo.

6.2. Uprawnienia osób, których dotyczą dane osobowe określone są art. 15-22 RODO i dotyczą:

1) prawa dostępu do danych;
2) prawa do sprostowania danych;
3) prawa do usunięcia danych;
4) prawa do ograniczenia przetwarzania;
5) prawa do przenoszenia danych;
6) prawa do sprzeciwu;

7) prawa by nie podlegać profilowaniu.

6.3. Administrator bez zbędnej zwłoki, nie później niż w terminie miesiąca od otrzymania żądania udziela osobie, której dane dotyczą informacji o działaniach podjętych w związku ze zgłoszonym żądaniem. W razie potrzeby termin ten może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. O takim przedłużeniu Administrator poinformuje osobę, której dane dotyczą w terminie miesiąca od otrzymania żądania i poda przyczyny opóźnienia.

6.4. Jeżeli Administrator nie podejmuje działań w związku ze zgłoszonym żądaniem (np. z uwagi na uznanie, że jest ono bezpodstawne), bez zbędnej zwłoki, nie później niż w terminie miesiąca od otrzymania żądania, udziela osobie, której dane dotyczą, informacji o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

6.5. Jeśli osoba, której dane dotyczą zgłosiła żądanie drogą elektroniczną, Administrator udzieli odpowiedzi w takiej samej formie, chyba, że osoba, której dane dotyczą zażądała odpowiedzi w innej formie.

6.6. W przypadku, gdy żądanie wpłynęło bezpośrednio do Osoby Upoważnionej, taka osoba niezwłocznie poinformuje Administratora o otrzymanym żądaniu i jego treści.

6.7. Administrator może zlecić Osobie Upoważnionej przygotowanie odpowiedzi na żądanie i podjęcie odpowiednich czynności.

6.8. Jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zwrócić się do niej o podanie dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

6.9. Osoba, której dane dotyczą ma prawo w dowolnym momencie wycofać swoją zgodę lub zgody na przetwarzanie danych osobowych. Wycofanie zgody lub zgód powinno zostać potwierdzone pisemnie lub za pośrednictwem poczty elektronicznej.

ROZDZIAŁ 7. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

7.1. Administrator może powierzyć podmiotowi trzeciemu przetwarzanie danych osobowych w imieniu Administratora.

7.2. W szczególności powierzenie przetwarzania danych osobowych może nastąpić na rzecz podmiotów świadczących usługi księgowe, HR, hostingowe, a także na rzecz podmiotów organizujących egzaminy językowe.

7.3. Powierzając przetwarzanie danych osobowych Administrator korzysta z usług Podmiotów Przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

7.4. Jeżeli Administrator ma wątpliwości co do spełnienia przez Podmiot Przetwarzający w/w warunków, może zwrócić się do niego o przedstawienie opisu zapewnianych gwarancji.

7.5. Administrator powierza przetwarzanie danych osobowych Podmiotom Przetwarzającym na podstawie umów, które określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą oraz obowiązki i prawa Administratora.

7.6. Umowy powierzenia przetwarzania danych zawierane będą w formie pisemnej lub elektronicznej.

7.7. Administrator prowadzi rejestr zawartych umów powierzenia. Wzór rejestru stanowi załącznik nr 4 do Polityki Bezpieczeństwa.

7.8. Administrator dokona weryfikacji projektu umowy powierzenia przetwarzania danych otrzymanego od podmiotu, który ma przetwarzać dane, pod kątem wymagań określonych w RODO i standardów stosowanych przez Szkołę lub przedstawi własny projekt spełniający w/w wymagania.

ROZDZIAŁ 8. RYZYKO NARUSZENIA OCHRONY DANYCH OSOBOWYCH

8.1. Administrator przyjmuje istnienie standardowego poziomu ryzyka naruszenia ochrony danych osobowych.

8.2. Ochrona danych osobowych może zostać naruszona w wyniku:

1) wystąpienia okoliczności losowych takich jak np. awarie oprogramowania zabezpieczającego, błąd Administratora lub Osoby Upoważnionej, zagubienie nośnika danych, jeśli był on niezabezpieczony;
2) wystąpienie okoliczności zamierzonych takich jak np. włamanie do systemu informatycznego, włamanie do Lokalu Szkoły, kradzież nośników danych.

8.3. Aby przeciwdziałać ewentualnym naruszeniom ochrony danych osobowych, zarówno spowodowanym okolicznościami losowymi jak i zamierzonymi, Administrator wprowadza środki techniczne i organizacyjne opisane w Polityce Bezpieczeństwa.

8.4. Po dokonaniu oceny treści obowiązujących przepisów prawa i zakresu przetwarzania danych osobowych Administrator uznał, że nie ma obowiązku wyznaczenia inspektora ochrony danych osobowych.

ROZDZIAŁ 9. PROCEDURA W PRZYPADKU NARUSZENIA OCHRONY DANYCH

9.1. Mając na celu zachowanie pełnej zgodności sposobu przetwarzania danych osobowych w Szkole z RODO, Administrator przyjmuje następującą procedurę wewnętrzną zgłaszania naruszenia ochrony danych osobowych organowi nadzoru.

9.2. Każda Osoba Upoważniona, która powzięła uzasadnione podejrzenie o możliwym naruszeniu ochrony danych osobowych przetwarzanych w Szkole, ma obowiązek natychmiastowego zawiadomienia Administratora o podejrzewanym naruszeniu.

9.3. Administrator w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je organowi nadzorczemu. Administrator może nie dokonać zgłoszenia, jeśli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W takim przypadku Administrator sporządza notatkę wskazującą na przyczyny niedokonania zgłoszenia.

9.4. Niezależnie od zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, Administrator podejmie czynności mające na celu ustalenie przyczyn naruszenia ochrony danych osobowych, a także osoby odpowiedzialne za zaistniałe naruszenie. W razie ustalenia takich osób Administrator podejmie dalsze stosowne kroki. Administrator podejmie również wszelkie niezbędne czynności mające na celu powstrzymanie niepożądanych skutków naruszenia ochrony danych osobowych.

9.5. Administrator prowadzi rejestr naruszeń ochrony danych osobowych w Szkole w oparciu o załącznik nr 7 do Polityki Bezpieczeństwa.

ROZDZIAŁ 10. POSTANOWIENIA KOŃCOWE

10.1. Polityka Bezpieczeństwa ma charakter dokumentu wewnętrznego i nie będzie udostępniana osobom trzecim, chyba że będzie to konieczne.

10.2. Administrator będzie dokonywał okresowej analizy Polityki Bezpieczeństwa pod kątem jej dostosowania do sposobów funkcjonowania Szkoły i przepisów prawa powszechnie obowiązującego.

10.3. Polityka Bezpieczeństwa będzie dostosowywana do bieżących potrzeb Administratora i przepisów prawa powszechnie obowiązującego, w przypadku, gdyby okazało się, że zasady ochrony danych osobowych w niej określone wymagają aktualizacji.

10.4. Załączniki stanowią integralną część Polityki Bezpieczeństwa.

10.5. Polityka Bezpieczeństwa została sporządzona w oparciu o stan prawny obowiązujący 5 kwietnia 2018 r.

ROZDZIAŁ 11. ZAŁĄCZNIKI

11.1. Upoważnienie do przetwarzania danych osobowych

11.2. Ewidencja Osób Upoważnionych

11.3. Formularz Zgłoszeniowy

11.4. Rejestr zawartych umów powierzenia przetwarzania danych

11.5. Wzory zgód na przetwarzanie danych osobowych

11.6. Rejestr czynności przetwarzania danych osobowych

11.7. Rejestr naruszeń ochrony danych osobowych