

Polityka bezpieczeństwa przetwarzania danych osobowych



Voice Productions Natalia Ojewska jako Global Education

Polityka Bezpieczeństwa i Ochrony Danych Osobowych (zwanej dalej „PB”) przetwarzanych przez Voice Productions Natalia Ojewska (zwanej Global Education) - została ustanowiona w oparciu o odpowiednie przepisy ustawy z 29.08.1997 roku o ochronie danych osobowych (tekst jednolity w Dz. U. z 16.12.2015 r., poz. 2135), zwanej dalej „u.o.d.o.”, oraz przepisy wykonawcze, w szczególności rozporządzenie ministra spraw wewnętrznych i administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zwane dalej Rozporządzeniem (Dz. U. z 29.04.2004 r., Nr 100, poz. 1024). Ilekroć inne, aniżeli powołane powyżej, przepisy prawa przewidują dalej idącą ochronę danych, w tym danych osobowych, te w zakresie zwiększonej ochrony mają zastosowanie. 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) PB ma zapewnić zgodne z prawem i wymaganiami odpowiednich umów przetwarzanie danych objętych regulacją PB, w tym danych osobowych. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. z 2015 r., poz. 745) w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji. Konstytucja Rzeczypospolitej Polskiej (art. 47, 51) ochrony i poszanowania życia prywatnego. Karta Praw Podstawowych Unii Europejskiej 2012/C 326/02 w szczególności art.8. Europejska Polityka dostępu do dokumentacji i archiwów 2004 R dotycząca tworzenia dokumentacji.

Polityka określa zakres bezpieczeństwa danych osobowych przetwarzanych przez Global Education. Osoby dopuszczone do przetwarzania danych osobowych przez bycie podmiotem, który przetwarza dane osobowe na rzecz Global Education lub osoby, którym zostają powierzone dane osobowe - zwane przetwarzającym w celach uzgodnionych z administratorem danych osobowych. Przetwarzanie danych osobowych dotyczy także pracowników zatrudnionych w Global Education. Wszystkie te osoby zostaną pouczone o warunkach i zasadach przetwarzania danych, w tym także o obowiązujących regulacjach prawnych i wewnętrznych Global Education.

Rozdział 1 - Postanowienia ogólne

§ 1.

Administratorem danych osobowych w GLOBAL EDUCATION jest Voice Productions Natalia Ojewska, ul. Targowa 46/5; 03-733 Warszawa.

§ 2

Celem Polityki bezpieczeństwa danych osobowych w firmie Global Education, zwanej dalej „Polityką Bezpieczeństwa”, jest uzyskanie odpowiedniego rozwiązania dla działań zgodnych z założeniami firmy, które są zgodne z wymogami obowiązujących aktów prawnych w Polsce oraz określają sposobu przetwarzania informacji zawierających dane osobowe. Dane jakie zbieramy są związane z rodzajem wykonywanej pracy w celach:

- konsultacji indywidualnych,
- doractwa edukacyjnego
- przygotowania do rekrutacji na studia za granicą,
- promocji edukacyjnej.

Nasze działania mają na celu pomóc w uzyskaniu najlepszego rozwiązania dla kandydatów na studentów zagranicą oraz dla studentów.

§ 3

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Global Education rozumiane jest jako zapewnienie rzetelności przetwarzania danych osobowych to znaczy zgodnie z obowiązującym prawem, w sposób przejrzysty, komunikatywny dla osób, których te dane dotyczą. Chcemy zapewnić poufność,

integralność, rozliczalność oraz dostępność danych osobowych na wysokim poziomie. Wyznacznikiem zapewniającym bezpieczeństwo danych jest oszacowanie ryzyka związanego z ochroną danych osobowych, gdzie będziemy się starać zminimalizować potencjalne zagrożenia.

2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
 - 1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom, podmiotom czy sztucznej inteligencji.
 - 2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione, naruszone lub zniszczone w sposób nieautoryzowany;
 - 3) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie zgodnie z obowiązującym prawem;
 - 4) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nie będą nieprzetwarzane dalej w sposób niezgodny z tymi celami;
 - 5) adekwatność - stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
 - 6) prawidłowe i w razie potrzeby uaktualniane;
 - 7) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiegokolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
 - 8) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
 - 9) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 4

1. Administratorem danych osobowych przetwarzanych w Global Education jest Voice Productions Natalia Ojewska.
2. Administrator danych decyduje o celach i środkach przetwarzania danych osobowych.
3. Administrator danych osobowych jest ich właścicielem.
4. Na administratorze danych osobowych spoczywają wszelkie obowiązki wynikające z przepisów prawa i to on decyduje o kształcie wewnętrznego systemu ochrony danych osobowych.

§ 5

Administrator danych osobowych jest zobowiązanych do ich chronienia, zabezpieczania, przez zniszczeniem lub utratą. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

Rozdział 2 - Definicje

§ 6

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

- 1) Administrator danych osobowych – Voice Productions Natalia Ojewska jako Global Education.
- 2) Inspektor danych osobowych – nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniami przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
- 3) Ustawa – rozumie się przez to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922);
- 4) Rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024);

- 5) Rozporządzenie Parlamentu Europejskiego i Rady (UE) (General Data Protection Regulation, GDPR) 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)
- 6) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- 7) Zbiór danych osobowych – każdy zbiór posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
- 8) Przetwarzane danych – rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
- 9) System informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
- 10) Platforma edukacyjna Global Education - interaktywny system komputerowy umożliwiający organizowanie i wsparcie nauczania w sieci Internetu. Do podstawowych funkcjonalności platformy edukacyjnej należą:
 - a. gromadzenie materiałów dydaktycznych
 - b. podział materiałów dydaktycznych na podstawie logicznych kryteriów ułatwiających zapoznanie się z materiałem
 - c. udostępnienie materiałów odbiorcom przez Internet
- 11) System tradycyjny – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
- 12) Zabezpieczenie danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem
- 13) użytkownik – rozumie się przez to upoważnionego przez administratora danych osobowych lub administratora bezpieczeństwa informacji (o ile został powołany), wyznaczonego do przetwarzania danych osobowych pracownika;
- 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

§ 7

1. W firmie Global Education przetwarzane są dane osobowe potrzebne przeprowadzenia konsultacji, aby pomóc aplikantowi w wyborze kierunków oraz uczelni, na które złoży podanie.
2. Podczas eventów edukacyjnych możemy zbierać dane podstawowe, które umożliwią nam kontakt w przyszłości z kandydatem na studenta.
3. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
4. Polityka bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

Rozdział 4 - Zasady przetwarzania danych

§ 8

1. Global Education dokłada wszelkich starań, by przetwarzane dane były przetwarzane zgodnie z obowiązującym prawem, z zapewnieniem maksymalnego poziomu bezpieczeństwa wszystkim podmiotom, których dane dotyczą. Przetwarzając dane ma na względzie w szczególności ochronę tych danych, zgodnie z

zasadami Polityka Bezpieczeństwa i obowiązującymi przepisami prawa. Ilekroć w Polityce Bezpieczeństwa mowa jest o przetwarzaniu danych przez Global Education, odpowiednie zapisy mają zastosowanie do wszystkich osób, które takie dane przetwarzają w ramach Global Education .

2. Global Education przetwarza dane osobowe, jeśli uzyskała zgodę osoby, której dane dotyczą, na przetwarzanie informacji o nim w celu i w zakresie, w jakim ta zgoda została udzielona. Global Education nie przetwarza danych w przypadku braku podstawy prawnej do ich przetwarzania.

§ 9

Politykę bezpieczeństwa stosuje się w szczególności do:

- 1) danych osobowych przetwarzanych w systemie: Microsoft Office 365 oraz w systemie CRM oraz WordPress, UCAS
- 2) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;
- 3) rejestru osób dopuszczonych do przetwarzania danych osobowych;
- 4) innych dokumentów zawierających dane osobowe.

§ 10

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki bezpieczeństwa mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:
 - 1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
 - 2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
2. Do stosowania zasad określonych przez dokumenty Polityki bezpieczeństwa zobowiązani są wszyscy pracownicy oraz inne osoby mające dostęp do informacji podlegających ochronie.

Rozdział 5 - Wykaz zbiorów danych osobowych

§ 11

1. Dane osobowe gromadzone są w zbiorach:

- 1) Pracownicy;
- 2) UCAS;
- 3) CRM
- 4) WordPress
- 5) Sync
- 6) Google Docs
- 7) Faktury;

§ 12

Zbiory danych osobowych wymienione w § 11 ust. 1 pkt 1 podlegają przetwarzaniu w sposób tradycyjny, które gromadzone są i przetwarzane przy użyciu systemu informatycznego i papierowego.

Rozdział 6

Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych -
ul. Targowa 46/5; 03-733 Warszawa - przechowywanie dokumentów.

§ 13

1. Dane osobowe przetwarzane są w budynku, ul. Targowa 46/5; 03-733 Warszawa. Siedziba skład się z jednego pomieszczenia w którym jest biuro z wydzieloną częścią oficjalną - salonem.

Rozdział 7

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych

§ 14

1. Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych jest bazą danych zamieszczoną w systemie CRM oraz WordPress, UCAS, Sync, Google Docs.
2. Także dane są zbierane podczas konsultacji w formie wywiadu. Te dane są zbierane w zbiory i przechowywane.

Rozdział 8 - Środki techniczne i organizacyjne zabezpieczenia danych osobowych

§ 15

1. Zabezpieczenia organizacyjne
 1. sporządzono i wdrożono Politykę bezpieczeństwa;
 2. do przetwarzania danych zostały dopuszczony jest wyłącznie administratora danych;
 3. stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
 4. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
 5. dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.
2. Zabezpieczenia techniczne
 1. komputer nie jest podłączany od sieci publicznej
 2. stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową - Kasperski;
 3. komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkownika i cykliczne wymuszanie zmiany hasła. Hasło będzie zmieniane nie rzadziej niż 30 dni. Komputer także jest zabezpieczony wygaszaczem na hasło.
 4. Dokumenty nieprzetwarzane zostaną zniszczone przy pomocy niszczarki.
3. Środki ochrony fizycznej:
 1. obszar, na którym przetwarzane są dane osobowe jest wprowadzona polityka kluczy - tylko osoby uprawnione do przebywania w pomieszczeniu;
 2. urządzenia służące do przetwarzania danych osobowych umieszcza się w zamkniętych pomieszczeniach;
 3. Dokumenty w formie papierowej będą zamknięte w szafce na klucz.
 4. Stosowana jest polityka czystego biurka - nie pozostawianie żadnych dokumentów z danymi osobowymi podczas nieobecności na biurku. Po zakończonej pracy należy uprzątnąć biurko z dokumentów papierowych oraz innych nośników informacji (płyty CD, DVD, pendrive itp.) przy stanowisku pracy.
 5. Polityka czystego ekranu - Komputer musi mieć ustawiony wygaszacz ekranu po podaniu hasła lub wyłączający się automatycznie po określonym czasie bezczynności użytkownika. Dodatkowo przed pozostawieniem włączonego komputera bez opieki użytkownicy powinni zablokować go (włączając wygaszacz ekranu) lub w przypadku dłuższej nieobecności wylogować się z systemu.
 6. Polityka czystego pulpitu - Na pulpicie komputera mogą znajdować się jedynie ikony standardowego oprogramowania i aplikacje służbowych oraz skróty folderów pod warunkiem, że w nazwie nie zawierają informacji o realizowanych projektach lub klientach.

7. Polityka czystych drukarek - Informacje drukowane powinny być zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby drukowania, użytkownik powinien skontaktować się z serwisantem odpowiedzialnym za poprawne funkcjonowanie urządzenia. Samodzielnie lub według instrukcji serwisanta usunąć informację z pamięci drukarki.
8. Polityka czystego kosza - Dokumenty papierowe z wyjątkiem materiałów promocyjnych, marketingowych i informacyjnych powinny być niszczone w sposób uniemożliwiający ich odczytanie, (najlepiej w niszczarce), umieszczane w specjalnie przeznaczonych do tego pojemnikach itp.
9. Kopie zapasowe:
 - a. przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
 - b. usuwa się niezwłocznie po ustaniu ich użyteczności.

Rozdział 9

§ 16

1. Corocznie do dnia 30 stycznia administrator danych przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych.
2. Sprawozdanie przygotowywane jest w formie pisemnej.
3. Na podstawie tego sprawozdania zostaną dane nie przetwarzane przenoszone do archiwum.

Rozdział 10 - Postanowienia końcowe

§ 17

1. Administrator danych osobowych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiegokolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.