POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH
BEST LINGUA Monika Mazur

	Data	Podpis
Opracowanie:	Maj 2018	
Zatwierdzenie:	01.06.2018	
Aktualizacja:	01.03.2023	
Aktualizacja:	16.03.2026	
Aktualizacja		

§ 1

Ilekroć w niniejszym dokumencie jest mowa o:

a) Przedsiębiorstwo – należy przez to rozumieć BEST LINGUA Monika Mazur; Nazwa skrócona BEST LINGUA;
b) Administrator Danych Osobowych – należy przez to rozumieć przedsiębiorstwo BEST LINGUA Monika Mazur, ul. Reformacka 6, 35-026 Rzeszów, NIP: 8161405781. BEST LINGUA jest podmiotem, który decyduje o środkach i celach przetwarzania danych osobowych swoich klientów, kontrahentów, współpracowników i pracowników oraz jest odpowiedzialny za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych;
c) Osoby przetwarzające dane – należy przez to rozumieć wszystkie osoby upoważnione do przetwarzania danych osobowych, czyli pracownika przedsiębiorstwa, osobę wykonującą pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej lub osobę odbywającą staż w przedsiębiorstwie;
d) Użytkownik systemu – należy przez to rozumieć osoby upoważnione przez Administratora Danych Osobowych do przetwarzania danych osobowych w systemie informatycznym przedsiębiorstwa. Użytkownikiem może być pracownik przedsiębiorstwa, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w przedsiębiorstwie lub wolontariusz, którzy zostali upoważnieni do dostępu do danych osobowych klientów, kontrahentów, współpracowników i pracowników przedsiębiorstwa;
e) Dane osobowe – wszelkie informacje umożliwiające zidentyfikowanie osoby fizycznej;
f) Przetwarzanie danych osobowych – operacje wykonywane na danych osobowych, polegające na zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu danych osobowych;
g) PUODO – Prezes Urzędu Ochrony Danych Osobowych;
h) RODO – przepisy dotyczące danych osobowych osób fizycznych, zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L. 2016.119.1);
i) Ustawa – ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (t.j. Dz. U. 2019, poz. 1781);
j) Polityka bezpieczeństwa przetwarzania danych BEST LINGUA Monika Mazur – zwana dalej „Polityką Bezpieczeństwa" jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu danych osobowych klientów, kontrahentów, współpracowników i pracowników BEST LINGUA Monika Mazur, zgodnie z przepisami RODO i Ustawy.

§ 2

1. Polityka Bezpieczeństwa wyznacza kierunek działania kierownictwa oraz pracowników przedsiębiorstwa w celu zapewnienia zgodnego z prawem przetwarzania danych osobowych oraz zapewnienia ich bezpieczeństwa przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.
2. Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z RODO, a także usprawnienie i usystematyzowanie organizacji pracy Administratora Danych Osobowych.
3. Realizując Politykę Bezpieczeństwa kierownictwo oraz pracownicy BEST LINGUA Monika Mazur dokładają szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewniają, aby dane te były:

a) przetwarzane zgodnie z prawem;
b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
c) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane;
d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

4. Zasady opisane w niniejszym dokumencie obowiązują wszystkie osoby przetwarzające dane osobowe w BEST LINGUA Monika Mazur.
5. Zasady opisane w niniejszym dokumencie obowiązują także podmioty przetwarzające dane osobowe na rzecz przedsiębiorstwa BEST LINGUA Monika Mazur, w zakresie określonym umową zawartą w tym przedmiocie. W szczególności podmioty te są zobowiązane do zachowania w tajemnicy informacji uzyskanych podczas powierzenia im zadań, w trakcie realizacji tych zadań oraz po ich zrealizowaniu.
6. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z Ustawy lub niniejszej Polityki Bezpieczeństwa, stosuje się w pierwszej kolejności przepisy tych ustaw.

§ 3

1. Polityka Bezpieczeństwa zawiera:
   a) ogólny opis systemu wraz ze zidentyfikowanymi i zastosowanymi mechanizmami bezpieczeństwa;
   b) określenie zasad ochrony danych osobowych zawartych w zbiorach danych, jak również poza nimi, przetwarzanych w systemach informatycznych oraz bez wykorzystania systemów informatycznych (tj. w rejestrach, ewidencjach, kartotekach, skorowidzach, wykazach itp.);
   c) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności przetwarzanych danych;
   d) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

§ 4

1. Administrator Danych Osobowych wykonuje wszelkie czynności i obowiązki wynikające z ustawy oraz aktów wykonawczych do ustawy, w szczególności:
   1) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych;
   2) wdraża dokumentację opisującą sposób przetwarzania danych, na którą składają się:
      a) Polityka bezpieczeństwa przetwarzania danych BEST LINGUA Monika Mazur;
      b) Instrukcja zarządzania systemem informatycznym BEST LINGUA Monika Mazur;
      c) Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych;
   3) ustala i wdraża środki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez nieuprawnioną osobę, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
   4) wydaje i odwołuje upoważnienia do przetwarzania danych osobowych pracowników;
   5) dopełnia obowiązku zgłaszania PUODO nowych i aktualizacji istniejących zbiorów danych osobowych;
   6) nadzoruje zasady ochrony danych osobowych.
2. Administrator Danych Osobowych może upoważnić do wydawania i odwoływania upoważnień do przetwarzania danych osobowych w Przedsiębiorstwie osoby spośród Członków Zarządu, jak również innego pracownika Przedsiębiorstwa.
3. Administrator Ochrony Danych powołuje Inspektora Danych Osobowych w sytuacjach, zgodnych z art. 37 ust. 1 RODO na podstawie właściwego upoważnienia, które może odwołać.

4. Administrator Danych Osobowych prowadzi rejestr upoważnień wydanych do przetwarzania danych osobowych w przedsiębiorstwie.
5. W przypadku nieobecności Administratora Danych Osobowych wyznacza on osobę go zastępującą.

§ 5

1. Administrator Danych Osobowych dokonuje kontroli i oceny funkcjonowania mechanizmów zabezpieczeń i ochrony.
2. Kontrole, o których mowa w ust. 1 nie mogą być dokonywane rzadziej niż raz do roku.
3. Przedmiotem kontroli, o której mowa w ust. 1 powinno być w szczególności:
   a) funkcjonowanie zabezpieczeń systemowych;
   b) prawidłowość funkcjonowania mechanizmów uwierzytelniania użytkowników;
   c) funkcjonowanie wprowadzonych zabezpieczeń fizycznych;
   d) realizacja wniosków osób, których prawa zostały uregulowane w RODO (np. prawo do zapomnienia, do ograniczenia przetwarzania i inne);
   e) realizacja procedur wdrożonych przez Administratora Danych Osobowych w zakresie ochrony danych osobowych;
   f) zasady przechowywania danych osobowych klientów, kontrahentów, współpracowników i pracowników przedsiębiorstwa BEST LINGUA Monika Mazur;
   g) zasady i sposoby likwidacji oraz archiwizowania danych osobowych.

§ 6

1. Dane osobowe przetwarzane w przedsiębiorstwie mogą być zbierane:
   a) bezpośrednio od osób, których te dane dotyczą lub
   b) z innych źródeł, w granicach dozwolonych przepisami prawa.
2. Dane osobowe klientów, kontrahentów, współpracowników i pracowników przedsiębiorstwa BEST LINGUA Monika Mazur są przetwarzane w celu wykonywania umowy lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, a także w celu wypełniania prawnych obowiązków ciążących na Administratorze Danych Osobowych, zgodnie z RODO.
3. Ponadto, w zbiorze danych mogą być przetwarzane dane osobowe klientów, kontrahentów, współpracowników i pracowników BEST LINGUA Monika Mazur w celu przesyłania newsletteru, oferty handlowej oraz prowadzenia działalności marketingowej.
4. Dane osobowe mogą być przetwarzane wyłącznie w celu, do którego zostały zebrane. Z zastrzeżeniem przepisów powszechnie obowiązujących oraz zobowiązań umownych, których stroną jest przedsiębiorstwo lub osoba fizyczna (w szczególności dotyczących archiwizacji dokumentów), po zrealizowaniu celu, dla jakiego dane były przetwarzane, dane te zostają trwale usunięte (zniszczone lub zmodyfikowane w sposób, który nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą).
5. Przetwarzanie danych osobowych nie może naruszać praw i wolności osób, których dane dotyczą, a w szczególności zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
6. W przedsiębiorstwie BEST LINGUA Monika Mazur gromadzone są następujące dane osobowe klientów, kontrahentów, współpracowników i pracowników:
   a) imię i nazwisko;
   b) data i miejsce urodzenia;
   c) adres zamieszkania (miejscowość, ulica, numer budynku, numer mieszkania, kod pocztowy);

d) adres do korespondencji (dane jw.);
e) dane przedsiębiorstwa prowadzonego przez osobę fizyczną;
f) numer telefonu;
g) adres e-mail;
h) nazwa zakładu pracy;
i) stanowisko;
j) doświadczenie zawodowe;
k) nr kont bankowych;
l) potwierdzenia wykształcenia, doświadczenia zawodowego, kwalifikacji i uprawnień.

§ 7

1. Przetwarzanie danych osobowych w BEST LINGUA Monika Mazur jest dopuszczalne tylko pod warunkiem przestrzegania właściwych przepisów prawnych.
2. Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych. Upoważnienie do przetwarzania danych osobowych może uzyskać wyłącznie osoba, która zapoznała się z przepisami Ustawy, RODO oraz zasadami ustalonymi w obowiązującej w przedsiębiorstwie dokumentacji opisującej sposób przetwarzania danych, o których mowa w § 4 ust. 1 pkt. 2).
3. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do niniejszej Polityki Bezpieczeństwa. Wzór odwołania upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 2 do niniejszej Polityki Bezpieczeństwa.
4. Dopuszcza się, aby dokument upoważnienia lub odwołania upoważnienia do przetwarzania danych osobowych obejmował więcej niż jedną osobę. Dopuszcza się także, aby dokument upoważnienia lub odwołania upoważnienia do przetwarzania danych osobowych odnosił się do dwóch lub większej liczby zbiorów danych osobowych.
5. Administrator Danych Osobowych jest odpowiedzialny za aktualność upoważnień wydanych osobom przetwarzającym dane osobowe w przedsiębiorstwie.
6. Z zastrzeżeniem ust. 7, przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu wyznaczonych. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których dopuszczalne jest przetwarzanie danych osobowych stanowi załącznik nr 3 do niniejszej Polityki Bezpieczeństwa. Wykaz jest sporządzany i aktualizowany na podstawie wiedzy i informacji powziętych przez Administratora Danych Osobowych.
7. W szczególnie uzasadnionych przypadkach dopuszczalne jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. przy użyciu urządzeń przenośnych lub elektronicznych nośników informacji), jednak wymaga to uprzedniej, pisemnej zgody Administratora Danych Osobowych. Szczegółowe zasady przetwarzania danych osobowych przy użyciu urządzeń przenośnych określone zostały w § 12 niniejszej Polityki Bezpieczeństwa.
8. Pomieszczenia znajdujące się w obszarze przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

§ 8

1. Dane osobowe przetwarzane przez przedsiębiorstwo udostępnia się wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów ustawy lub innych przepisów powszechnie obowiązujących.
2. Z zastrzeżeniem ust. 3, dane osobowe udostępnia się na umotywowany wniosek, chyba że odrębne przepisy stanowią inaczej.
3. Dane osobowe mogą zostać udostępnione także na wniosek (za zgodą) osoby, której dane dotyczą.
4. Wniosek, o którym mowa w ust. 3, powinien zawierać co najmniej określenie:
    a) wnioskodawcy;

b) podstawy żądania udostępnienia danych (wykazanie przez wnioskodawcę zasadności udostępnienia danych);
c) zakresu żądanej informacji.

5. W przypadku uzasadnionego wniosku, dane osobowe udostępnia Administrator Danych Osobowych lub inny upoważniony do tego pracownik. W przypadku uzasadnionych wątpliwości co do zasadności udostępnienia danych osobowych, Administrator Danych Osobowych może wystąpić o zajęcie stanowiska przez PUODO.
6. Administrator Danych Osobowych prowadzi ewidencję wniosków o udostępnienie danych osobowych, stanowiących załącznik nr 6 niniejszej Polityki Bezpieczeństwa.
7. Z zastrzeżeniem ust. 8 oraz przypadków określonych w przepisach powszechnie obowiązujących, przed udostępnieniem (w tym opublikowaniem) znajdujących się w posiadaniu przedsiębiorstwa dokumentów lub informacji, zawierających dane osobowe, które nie mają bezpośredniego związku z celem udostępnienia, należy z dokumentu lub informacji trwale usunąć dane osobowe (lub trwale zmodyfikować dane osobowe) w taki sposób, aby niemożliwe było ustalenie tożsamości osoby, której dane dotyczą (anonimizacja danych), np. przez trwałe zaczernienie danych osobowych, zastąpienie danych osobowych wielokropkiem lub pojedynczą literą.
8. Udostępnienie (w tym publikacja) znajdujących się w posiadaniu Administratora Danych Osobowych dokumentów lub informacji zawierających dane osobowe jest dopuszczalne także po uzyskaniu zgody osoby, której dane zawiera dokument.

§ 9

1. Przedsiębiorstwo może powierzyć przetwarzanie danych osobowych, których jest administratorem innemu podmiotowi wyłącznie na podstawie umowy zawartej w formie pisemnej.
2. W umowie powierzenia przetwarzania danych osobowych należy zobowiązać podmiot przyjmujący dane do przetwarzania do:
    a) przetwarzania danych osobowych wyłącznie w zakresie i w celu określonym w umowie;
    b) zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych, określonych w przepisach o ochronie danych osobowych;
    c) zachowania w tajemnicy informacji uzyskanych w związku z realizacją powierzonych mu zadań, w trakcie realizacji umowy oraz po ich wykonaniu;
    d) wykonywania innych obowiązków w zakresie ochrony danych osobowych w imieniu i na rzecz przedsiębiorstwa (np. wydawania upoważnień pracownikom podmiotu przyjmującego dane do przetwarzania).

§ 10

1. Możliwe jest przetwarzanie w przedsiębiorstwie danych osobowych powierzonych przez inny podmiot (zleceniodawcę, podmiot powierzający).
2. W przypadku, o którym mowa w ust. 1 przetwarzanie danych osobowych odbywa się na podstawie umowy zawartej w formie pisemnej pomiędzy przedsiębiorcą a zleceniodawcą (podmiotem powierzającym).
3. W umowie w sprawie powierzenia przetwarzania danych osobowych każdorazowo określone zostaną zakres powierzanych danych i cel w jakim dane mogą być przetwarzane. Przetwarzanie danych dopuszczalne jest tylko w określonym w umowie zakresie i celu.
4. Powierzone dane podlegają ochronie na takich samych zasadach jak dane, których Administratorem w rozumieniu Ustawy jest BEST LINGUA Monika Mazur, chyba że umowa określi inne zasady ochrony danych osobowych.

§ 11

Przedsiębiorstwo wprowadza następujące minimalne środki techniczne i organizacyjne niezbędne do zapewnienia poufności przetwarzanych danych:

1. Środki ochrony fizycznej:

a) budynek użyteczności publicznej, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest wyposażony w alarm;

b) drzwi wejściowe do budynku posiadają zamki patentowe;

c) dostęp do pomieszczeń, w których przetwarzane są dane osobowe jest niedostępny dla osób do tego nieupoważnionych;

d) urządzenia służące do przetwarzania danych osobowych znajdują się w wydzielonych pomieszczeniach;

e) zbiory danych prowadzone w formie tradycyjnej (tj. mające postać papierowych rejestrów, ewidencji, kartotek, skorowidzów, wykazów itp.), są przechowywane pod zamknięciem, w zamykanych szafach i pokojach;

f) przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby upoważnionej do przetwarzania danych lub w obecności Administratora Danych Osobowych;

g) pomieszczenia, o których mowa wyżej, są zamykane na czas nieobecności ADO lub pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich;

h) w przypadku przebywania interesantów bądź innych osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych ustawione są w taki sposób, że uniemożliwiają tym osobom wgląd w dane;

i) nie jest dopuszczalne przeglądanie dokumentacji papierowej lub elektronicznej związanej z danymi osobowymi przy osobach do tego nieupoważnionych.

2. Środki sprzętowe, informatyczne i telekomunikacyjne:

a) każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia jest niszczony w sposób uniemożliwiający jego odczytanie;

b) na stanowiskach pracy, w których przetwarzane są dane osobowe zainstalowano zaporę sieciową, system antywirusowy, poczta elektroniczna wpływająca do przedsiębiorstwa skanowana jest programem antywirusowym;

c) dane osobowe w systemach informatycznych mogą być przetwarzane na pojedynczych stanowiskach komputerowych lub na stanowiskach sieciowych podłączonych do serwera Przedsiębiorstwa;

d) urządzenia przenośne lub elektroniczne nośniki informacji mogą być wykorzystywane do przetwarzania danych osobowych poza obszarem przetwarzania danych jedynie w uzasadnionych wypadkach, po uzyskaniu zgody Administratora Danych Osobowych, na zasadach określonych w § 12 niniejszej Polityki Bezpieczeństwa.

3. Środki ochrony w ramach oprogramowania systemu:

a) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelniania z wykorzystaniem hasła lub PIN.

4. Środki ochrony w ramach systemu użytkowego:

a) zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika;

b) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego w przypadku dłuższej nieaktywności pracy użytkownika;

c) komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem wejściowym do systemu operacyjnego;

d) sporządza się kopie zapasowe nie rzadziej niż raz na miesiąc.

5. Środki organizacyjne:

a) bezpośredni nadzór nad przetwarzaniem danych osobowych oraz nad zbiorami danych osobowych sprawuje Administrator Danych Osobowych;
b) do przetwarzania danych osobowych może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych;
c) każda osoba przed uzyskaniem dostępu do danych osobowych przetwarzanych w przedsiębiorstwie obowiązana jest zapoznać się z przepisami Ustawy i Rozporządzenia RODO oraz Polityką Bezpieczeństwa, Instrukcją zarządzania systemem informatycznym BEST LINGUA Monika Mazur oraz Instrukcją postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych. Fakt ten potwierdza pisemnym oświadczeniem oraz zobowiązuje się do przestrzegania zasad, reguł i postanowień z nich wynikających oraz zachowania tajemnicy. Wzór oświadczenia stanowi załącznik nr 4 do niniejszej Polityki Bezpieczeństwa;
d) osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do pracy zostaną przeszkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz poinformowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym;
e) w przypadku zaprzestania przetwarzania danych osobowych przez osobę do tego upoważnioną, Administrator Danych Osobowych zobowiązany jest do odwołania udzielonego upoważnienia, zgodnie ze wzorem stanowiącym załącznik nr 2 do niniejszej Polityki Bezpieczeństwa;
f) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik nr 5 do niniejszej Polityki Bezpieczeństwa;
g) prowadzona jest ewidencja wniosków o udostepnienie danych osobowych zgodnie ze wzorem stanowiącym załącznik nr 6 do niniejszej Polityki Bezpieczeństwa;
h) prowadzona jest ewidencja umów powierzenia przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik nr 7 do niniejszej Polityki Bezpieczeństwa;
i) stosuje się pisemne umowy powierzenia przetwarzania danych dla podmiotów, którym powierza się przetwarzanie danych osobowych klientów, kontrahentów, współpracowników i pracowników przedsiębiorstwa BEST LINGUA Monika Mazur;
j) wprowadzono Instrukcję zarządzania systemem informatycznym BEST LINGUA Monika Mazur oraz Instrukcję postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych;
k) z zastrzeżeniem §12, przetwarzanie danych osobowych jest dozwolone tylko w pomieszczeniach wskazanych w załączniku nr 3 do niniejszej Polityki Bezpieczeństwa (w obszarze przetwarzania danych);
l) w podmiocie prowadzi się politykę czystego biurka i ekranu.
m) Zabezpieczenie systemu informatycznego, w zakresie nieuwzględnionym w niniejszej Polityce Bezpieczeństwa, reguluje Instrukcja zarządzania systemem informatycznym BEST LINGUA Monika Mazur.

§ 12

1. Przetwarzanie danych osobowych z wykorzystaniem przenośnych urządzeń elektronicznych, czyli nośników informacji (laptop, pendrive, kart pamięci, dysków zewnętrznych i innych zewnętrznych nośników informacji) powinno być ograniczone do niezbędnych przypadków.
2. Przetwarzanie danych osobowych z wykorzystaniem urządzeń przenośnych lub elektronicznych nośników informacji poza budynkami przedsiębiorstwa, zgodnie z wykazem stanowiącym załącznik nr 3 do niniejszej Polityki Bezpieczeństwa może odbywać się wyłącznie za uprzednią pisemną zgodą Administratora Danych Osobowych, w której zatrudniony jest pracownik korzystający z urządzenia przenośnego lub elektronicznego nośnika informacji.
3. Zgoda, o której mowa w ust. 2, określa:

a) zakres danych osobowych, które mają być przetwarzane na urządzeniu przenośnym lub elektronicznym nośniku informacji;

b) okres, w którym niezbędne jest korzystanie do przetwarzania danych osobowych z urządzenia przenośnego lub elektronicznego nośnika informacji;
c) imię i nazwisko osoby będącej użytkownikiem urządzenia przenośnego lub elektronicznego nośnika informacji;
d) uzasadnienie potrzeby przetwarzania danych osobowych przy użyciu urządzenia przenośnego lub elektronicznego nośnika informacji;
e) w przypadku przetwarzania danych osobowych przy użyciu urządzenia przenośnego: nazwę systemu informatycznego służącego do przetwarzania danych osobowych oraz model/typ i numer seryjny urządzenia.

4. Osoba korzystająca z urządzenia przenośnego w celu przetwarzania danych osobowych poza budynkiem przedsiębiorstwa, odpowiada za prawidłowe zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem. Użytkownik urządzenia przenośnego zobowiązany jest w szczególności do:

a) korzystania z urządzenia w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z urządzenia w miejscach publicznych i w środkach transportu publicznego;
b) niedopuszczania do korzystania z urządzenia przenośnego przez osoby nieupoważnione;
c) zabezpieczania urządzenia przenośnego hasłem;
d) blokowania dostępu do urządzenia przenośnego w przypadku, gdy nie jest ono wykorzystywane przez upoważnionego użytkownika;
e) zapewnienia aktualizacji oprogramowania antywirusowego.

5. W razie utraty urządzenia przenośnego lub elektronicznego nośnika informacji wykorzystywanego do przetwarzania danych osobowych, użytkownik urządzenia lub nośnika zobowiązany jest do natychmiastowego powiadomienia Administratora Danych Osobowych.

§ 13

Każda osoba przetwarzająca dane osobowe jest zobowiązana powiadomić Administratora Danych Osobowych o naruszeniach bezpieczeństwa systemu ochrony danych osobowych. Tryb postępowania określa Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.

§ 14

1. Osoba, która:
    1) przetwarza w zbiorze danych:
        a) dane osobowe, do których przetwarzania nie jest upoważniona;
        b) dane osobowe, których przetwarzanie nie jest dopuszczalne;
    2) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;
    3) narusza choćby nieumyślnie obowiązek zabezpieczenia danych przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem;
    4) nie zgłasza zbiorów danych podlegających rejestracji;
    5) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;
    6) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw;
    7) udaremnia lub utrudnia Inspektorowi Urzędu Ochrony Danych Osobowych wykonanie czynności kontrolnej

podlega odpowiedzialności karnej przewidzianej w ustawie o ochronie danych osobowych oraz odpowiedzialności służbowej i dyscyplinarnej przewidzianej w Kodeksie pracy.

2. Osoba, która narusza w inny sposób przepisy Ustawy, Rozporządzenia RODO, niniejszej Polityki Bezpieczeństwa oraz obowiązujących w przedsiębiorstwie instrukcji zarządzania systemem informatycznym BEST LINGUA Monika Mazur, czy Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych, podlega odpowiedzialności służbowej i dyscyplinarnej przewidzianej w Kodeksie pracy.

3. Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych i ich zabezpieczenie są:
    a) upoważnione osoby do przetwarzania danych osobowych;
    b) Administrator Danych Osobowych.

§ 15

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy BEST LINGUA Monika Mazur.

Zatwierdzam
Monika Mazur
Administrator Danych Osobowych