POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

FIRMA HANDLOWO-USŁUGOWA „MIKADO" IMPORT-EKSPORT z siedzibą w OBORNIKACH

Zgodna z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s.1)

Spis treści

POLITYKA OCHRONY DANYCH OSOBOWYCH

1 Podstawa prawna

Niniejszy dokument jest polityką ochrony danych osobowych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1), zwanego dalej: *RODO.*

2 Definicja, cele, założenia i zakresstosowania Polityki ochrony danych osobowych

2.1 Definicja

2.1.1 Niniejsza Polityka ochrony danych osobowych (zwana dalej: *Polityką*) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Firmie Handlowo-Usługowej „Mikado" Import-Export z siedzibą w Obornikach, zwanego dalej: *Administratorem*.

2.1.2 Polityka składa się z:

2.1.2.1 opisu zasad ochrony danych osobowych, obowiązujących u Administratora;

2.1.2.2 załączników uszczegóławiających i uzupełniających niniejszą Politykę.

2.2 Cele

Celem Polityki Bezpieczeństwa Informacji jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonywać obowiązki Administratora w zakresie bezpieczeństwa danych osobowych.

2.2.1 W szczególności do celów Polityki należy:

2.2.1.1 zabezpieczenie zasobów systemów, infrastruktury technicznej, sprzętu i osprzętu przed kradzieżą, zniszczeniem lub uszkodzeniem,

2.2.1.2 uniemożliwienie instalowania i posługiwania się oprogramowaniem nielegalnym lub niebezpiecznym,

2.2.1.3 uniemożliwienie dostępu do informacji zawartych w systemach informatycznych osobom do tego nie upoważnionym,

2.2.1.4 uniemożliwienie zniszczenia lub nieuprawnionej zmiany danych osobowych,

2.2.1.5 zabezpieczenie dokumentacji papierowej zawierające dane osobowe przed ich kradzieżą lub kopiowaniem.

2.3 Założenia

2.3.1 Ochrona danych osobowych u Administratora opiera się na następujących filarach:

2.3.1.1 Zgodności z prawem – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

2.3.1.2 Bezpieczeństwa – Administrator dokłada wszelkich starań, aby zapewnić odpowiedni poziom bezpieczeństwa danych.

2.3.1.3 Praw osób, których dane dotyczą – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

2.3.1.4 Rozliczalności – Administrator dokumentuje to, w jaki sposób wywiązuje się z ciążących na nim obowiązków ochrony danych osobowych, aby w każdej chwili móc wykazać zgodność przetwarzania danych osobowych z RODO.

2.4 Zasady

2.4.1 Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:

2.4.1.1 Zgodności z prawem – dane osobowe przetwarzane są w oparciu o konkretną podstawę prawną i zgodnie z prawem;

2.4.1.2 Rzetelności – dane osobowe przetwarzane są rzetelnie i uczciwie;

2.4.1.3 Przejrzystości – dane osobowe przetwarzane są w sposób przejrzysty dla osoby, której dane dotyczą;

2.4.1.4 Minimalizacji – dane osobowe przetwarzane są wyłącznie w zakresie niezbędnym do celów;

2.4.1.5 Adekwatności – przetwarzanie danych osobowych jest proporcjonalne do potrzeb Administratora;

2.4.1.6 Ograniczoności przechowywania – dane są przechowywane przez Administratora przez okres nie dłuższy niż niezbędne jest to do celów, w których dane te są przetwarzane;

2.4.1.7 Prawidłowości – przetwarzanie danych osobowych odbywa się z dbałością o prawidłowość danych osobowych;

2.4.1.8 Czasowości – przetwarzanie danych osobowych odbywa się w koniecznym czasie;

2.4.1.9 Integralności i poufności – Administrator zapewnia odpowiednie bezpieczeństwo przetwarzania danych osobowych.

2.5 Zakres stosowania Polityki

2.5.1 Zasady określone przez Politykę mają zastosowanie do wszystkich zbiorów danych osobowych administrowanych przez Administratora, w szczególności do:

2.5.1.1 wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą dane osobowe podlegające ochronie;

2.5.1.2 danych osobowych przetwarzanych przez Administratora zarówno w przypadku, gdy jest on administratorem danych, jak i w sytuacji, gdy przetwarza dane powierzone mu na podstawie umów powierzenia przetwarzania danych osobowych, w rozumieniu art. 28 RODO;

2.5.1.3 wszystkich nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe podlegające ochronie;

2.5.1.4 wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe podlegające ochronie;

2.5.1.5 wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do danych osobowych podlegających ochronie.

2.5.2 Do stosowania zasad określonych przez Politykę zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy, konsultanci, stażyści i inne osoby mające dostęp do informacji podlegających ochronie.

3 Terminologia

1. Administrator Danych Osobowych (*Administrator*) – Firma Handlowo-Usługowa „Mikado" Import-Eksport z siedzibą w Obornikach, wpisana do Centralnej Ewidencji i Informacji o Działalności Gospodarczej prowadzonej przez Ministra Gospodarki pod adresem: ul. Objezierska 3, 64-600 Oborniki, NIP: 787-121-33-46, REGON: 631180551.
2. Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. Zbiór danych osobowych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
4. Przetwarzanie danych osobowych – 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;
5. Użytkownik – osoba mająca dostęp do zasobów systemu informatycznego posiadająca upoważnienie do przetwarzania danych osobowych w tym systemie;
6. System informatyczny – zespół urządzeń, sprzętu komputerowego, oprogramowania oraz baz danych przetwarzających dane osobowe;
7. Nośniki danych – wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski, dyskietki, dyski CD-ROM, karty magnetyczne lub pamięci przenośne;
8. Sieć informatyczna – fizyczna warstwa systemu informatycznego obejmująca okablowanie, węzły i urządzenia aktywne organizujące ruch w sieci;
9. Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, który przetwarza dane osobowe w imieniu administratora na mocy umowy powierzenia przetwarzania danych osobowych, zgodnie z art. 28 RODO.

4 System ochrony danych osobowych u Administratora:

4.1 Inwentaryzacja danych osobowych

4.1.1 Administrator dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w szczególności: przypadków przetwarzania danych wrażliwych, przypadków przetwarzania danych niezidentyfikowanych, przypadków przetwarzania danych dzieci; profilowania.

4.1.2 Administrator weryfikuje czy dochodzi do przypadków współadministrowania danymi osobowymi.

4.2 Rejestr Czynności Przetwarzania Danych Osobowych

4.2.1 Administrator prowadzi Rejestr Czynności Przetwarzania Danych Osobowych, zwany dalej: *Rejestrem*.

4.2.2 W Rejestrze, dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, odnotowuje co najmniej: (i) nazwę czynności, (ii) cel przetwarzania, (iii) opis kategorii osób, (iv) opis kategorii danych, (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora, jeśli podstawą jest uzasadniony interes, (vi) sposób zbierania danych, (vii) opis kategorii odbiorców danych (w tym przetwarzających), (viii) informację o przekazaniu poza EU/EOG; (ix) ogólny opis technicznych i organizacyjnych środków ochrony danych.

4.2.3 Wzór Rejestru stanowi Załącznik nr 2 do Polityki. Wzór Rejestru zawiera kolumny nieobowiązkowe. W kolumnach nieobowiązkowych rejestruje się informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych osobowych.

4.3 Podstawy prawne przetwarzania danych osobowych

4.3.1 Administrator identyfikuje i weryfikuje podstawy prawne przetwarzania danych osobowych, a w szczególności:

4.3.1.1 utrzymuje system zarządzania zgodami na przetwarzanie danych osobowych;

4.3.1.2 inwentaryzuje i przygotowuje uzasadnienia przypadków, gdy dochodzi do przetwarzania danych osobowych na podstawie prawnie uzasadnionych interesów Administratora.

4.3.2 Administrator rejestruje podstawy prawne przetwarzania danych osobowych w Rejestrze.

4.4 Prawa osoby, której dane dotyczą

4.4.1 Administrator wywiązuje się z obowiązków informacyjnych względem osób, których dane dotyczą. W szczególności Administrator:

4.4.1.1 przekazuje osobom, których dane dotyczą wszelkie wymagane prawem informacje w czasie pozyskiwania danych osobowych, jak również w innych sytuacjach, gdy prawo wymaga przekazania dodatkowych informacji osobom, których dane dotyczą;

4.4.1.2 zapewnia dokumentację realizacji obowiązków, o których mowa w pkt. 4.4.1.1.

4.4.2 Administrator zapewnia osobom, których dotyczą realizację praw przysługujących im na podstawie RODO. W szczególności Administrator dokłada starań, aby żądania osób, których dane dotyczą były realizowane w terminach wyznaczonych przez RODO oraz rzetelnie dokumentowane.

4.4.3 Administrator stosuje procedury działania w przypadku naruszenia ochrony danych osobowych, pozwalające na identyfikację i weryfikację naruszenia, a w razie potrzeby jego niezwłoczne zgłoszenie Urzędowi Ochrony Danych Osobowych oraz zawiadomienie osoby, której dane dotyczą.

4.5 Minimalizacja

4.5.1 Administrator stosuje metodykę zarządzania minimalizacją (*privacy by default*), która ustala zasady: zarządzania adekwatnością danych, reglamentacji i zarządzania dostępem do danych, zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

4.6 Bezpieczeństwo danych osobowych

4.6.1 Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania.

4.6.2 Administrator ustala przydatność oraz stosuje takie środki i podejście jak:

4.6.2.1 pseudonimizacja,

4.6.2.2 szyfrowanie danych osobowych,

4.6.2.3 inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

4.6.2.4 środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

4.6.3 Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

4.6.3.1 przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

4.6.3.2 przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

4.6.3.3 dostosowuje środki ochrony danych do ustalonego ryzyka;

4.6.3.4 wdraża system zarządzania bezpieczeństwem informacji;

4.6.3.5 zarządza incydentami naruszenia ochrony danych osobowych.

4.7 Zasady powierzania danych osobowych podmiotom przetwarzającym

4.7.1 Powierzenie przetwarzania danych osobowych podmiotom przetwarzającym następuje w drodze umowy zawartej na piśmie.

4.7.2 Umowa powierzenia przetwarzania danych osobowych stanowi Załącznik nr 3 do Polityki.

4.8 Przekazywanie danych osobowych

4.8.1 Administrator na bieżąco weryfikuje czy dane osobowe nie są przekazywane do państw trzecich (tj. poza Europejski Obszar Gospodarczy) lub do organizacji międzynarodowych.

4.8.2 W przypadku przekazywania danych osobowych do państw trzecich lub do organizacji międzynarodowych Administrator zapewnia zgodność przekazywania danych z RODO.

4.8.3 Administrator na bieżąco weryfikuje, czy zachodzą przypadki transgranicznego przetwarzania danych osobowych.

4.9 Privacy by design

4.9.1 Administrator uwzględnia ochronę danych osobowych w fazie projektowania.

4.10 Wykaz budynków oraz pomieszczeń, w których przetwarzane są dane osobowe

4.10.1 Obszary przetwarzania danych osobowych określa załącznik nr 5 do Polityki.

4.11 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania

4.11.1 Wykaz zbiorów danych osobowych, opis ich struktury wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy systemami, a także wskazanie programów stosowanych do przetwarzania danych osobowych określa załącznik nr 10 do Polityki.

5 Postanowienia końcowe

5.1 Procedury nadawania uprawnień, metody i środki uwierzytelnienia oraz procedury tworzenia kopii zapasowych reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

5.2 Aktualizacji niniejszej Polityki dokonuje Administrator, który wszelkie propozycje zmian przedstawia podmiotowi odpowiedzialnemu za jej wdrożenie.

5.3 Niniejsza Polityka wchodzi w życie z dniem [07.06. 2018].