POLITYKA BEZPIECZEŃSTWA

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

A. POSTANOWIENIA OGÓLNE

§ 1. Podstawy prawne

1. W celu zapewnienia ochrony przetwarzanych danych osobowych Właściciel wprowadza „Politykę bezpieczeństwa danych osobowych”.
2. Podstawą prawną instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych są art. 36 ust. 2 w zw. z art. 3 ust. 2 punkt 2 ustawy odo oraz § 3 i § 4 Rozporządzenia.

§ 2. Definicje

Terminy użyte w niniejszym dokumencie oznaczają:

1. Polityka bezpieczeństwa: niniejsza „Polityka bezpieczeństwa danych osobowych”;
2. Właściciel lub Administrator danych: EMPRO Marcin Masny, ul. Targowa 60, 08-400 Garwolin, prowadzący działalność gospodarczą pod firmą EMPRO Marcin Masny, NIP: 826-154-49-09, Regon: 712561782;
3. Dane osobowe lub dane: wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4. Ustawa odo: ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. 2014.1182 ze zm.);
5. Rozporządzenie: rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U.2004.100.1024);
6. Kodeks pracy: ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. 2014.1502 ze zm.).

§ 3. Zagadnienia organizacyjne

1. Dane osobowe przetwarzane są w związku z działalnością gospodarczą Właściciela. W szczególności dane osobowe przetwarza się:
   1. w celu zapewnienia prawidłowej, zgodnej z prawem i celami Właściciela polityki personalnej oraz bieżącej obsługi stosunków pracy;
   2. w związku ze świadczeniem Właścicielowi lub przez Właściciela usług na podstawie umów cywilnoprawnych,
   3. w celu wystawienia faktury, rachunku w związku z zawieraniem i wykonywaniem umów cywilnoprawnych zawieranych przez Właściciela w ramach prowadzenia działalności gospodarczej,
   4. w celu prowadzenia dokumentacji księgowej lub sprawozdawczości finansowej;
   5. dla realizacji innych usprawiedliwionych celów i zadań Właściciela – z poszanowaniem praw i wolności osób powierzających Właścicielowi swoje dane.
2. Polityka bezpieczeństwa odnosi się do danych osobowych przetwarzanych w zbiorach danych:
   1. tradycyjnych, w szczególności w aktach osobowych i w innych zbiorach ewidencyjnych,
   2. w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
3. Dane osobowe u Właściciela przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
   1. przepisów ustawy odo oraz przepisów wykonawczych z nią związanych, w tym Rozporządzenia,
   2. przepisów art. 221 §1 – 4 kodeksu pracy,
   3. innych przepisów ustaw i rozporządzeń normujących przetwarzanie danych osobowych.

§ 4. Podstawowe założenia i cele

1. Właściciel dokłada należytej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1. przetwarzane zgodnie z prawem,
2. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
3. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
4. przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

2. Właściciel stosuje odpowiednie środki informatyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności:
   1. przed ich udostępnieniem osobom nieupoważnionym,
   2. przed zabraniem przez osobę nieuprawnioną,
   3. przetwarzaniem z naruszeniem przepisów prawa,
   4. zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. Właściciel dąży do systematycznego unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych. W szczególności, Właściciel zapewnia aktualizacje informatycznych środków ochrony danych osobowych pozwalającą na zabezpieczenie przed wirusami, nieuprawnionym dostępem oraz inni zagrożeniami danych, płynącymi z funkcjonowania systemu informatycznego oraz sieci telekomunikacyjnych.

B. PROCEDURY

§ 5. Uprawnienia i dostęp do danych

1. Właściciel udostępnia przetwarzane na jego obszarze dane osobowe wyłącznie osobom do tego upoważnionym na mocy obowiązujących uregulowań wewnętrznych.
2. Upoważnienie może być udzielone, jeśli potrzeba taka wynika z:
   1. charakteru pracy wykonywanej na danym stanowisku pracy lub świadczonych usług, lub
   2. dokumentu określającego zakres obowiązków (zakres czynności) wykonywanych

na danym stanowisku pracy, lub

3. odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych. Wzór upoważnienia stanowi załącznik nr 1 do Polityki bezpieczeństwa.

3. Właściciel zapewnia dostęp do przetwarzanych danych osobowych osobom fizycznym będącym dysponentami tych danych.
4. Dysponentami danych osobowych są osoby, które powierzyły swoje dane w związku z zatrudnieniem lub na podstawie innych stosunków cywilnoprawnych.
5. Osoby niezatrudnione przy przetwarzaniu danych osobowych określonej kategorii, w tym dysponenci danych osobowych, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych mogą mieć do nich wgląd wyłącznie w obecności upoważnionego przedstawiciela Właściciela lub Właściciela.
6. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia Administratora danych może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii, w szczególności Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Agencja Bezpieczeństwa Wewnętrznego, Wojskowe Służby Informacyjne, sady powszechne, Najwyższa Izba Kontroli, Generalny Inspektor Ochrony Danych Osobowych i inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień – po okazaniu dokumentów potwierdzających te uprawnienia.

§ 6. Przetwarzanie danych

1. Właściciel dopuszcza do przetwarzania danych wyłącznie osoby posiadające upoważnienie nadane przez Właściciela.
2. Upoważnienie może być udzielone, jeśli potrzeba taka wynika z:
   1. charakteru pracy wykonywanej na danym stanowisku pracy lub świadczonych usług, lub
   2. dokumentu określającego zakres obowiązków (zakres czynności) wykonywanych na danym stanowisku pracy, lub
   3. odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych. Wzór upoważnienia stanowi załącznik nr 2 do Polityki

bezpieczeństwa.

3. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która zawiera:
   1. imię i nazwisko osoby upoważnionej,
   2. datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
   3. identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
4. Ewidencja osób upoważnionych stanowi załącznik nr 3 do Polityki bezpieczeństwa.
5. Osoby upoważnione do przetwarzania danych osobowych zostają zaznajomione z zakresem informacji objętych tajemnicą w związku z wykonywaną przez siebie pracą. W szczególności są one informowane o powinności zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Osoby upoważnione do przetwarzania danych są obowiązane zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia.
6. Właściciel zapewnia zaznajomienie osób upoważnionych do dostępu i/lub przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także stosowanymi technikami i środkami ochrony tych danych.

§ 7. Prawa osób, których dane są przetwarzane

1. Właściciel gwarantuje realizacje uprawnień gwarantowanych przez obowiązujące przepisy prawa osobom fizycznym, których dane osobowe są przetwarzane – z poszanowaniem praw i wolności osób powierzających swoje dane.
2. W szczególności każdej osobie fizycznej, której dane osobowe są przetwarzane, przysługuje prawo do uzyskania informacji o zakresie jej uprawnień związanych z ochroną danych osobowych, a także prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych na zasadach określonych w art. 32 – 35 ustawy odo.
3. Administrator danych jest obowiązany poinformować osobę, której dane dotyczą – na jej wniosek – o przysługujących jej prawach oraz udzielić informacji:

1. jakie dane osobowe zawiera zbiór,
2. w jaki sposób zebrano dane,
3. w jakim celu i zakresie dane są przetwarzane,
4. w jakim zakresie oraz komu dane zostały udostępnione.

§ 8. Usuwanie i niszczenie

1. Właściciel sprawuje kontrolę i nadzór nad usuwaniem zbędnych danych osobowych i/lub ich zbiorów i niszczeniem ich nośników. Kontrola i nadzór może polegać na wprowadzeniu odpowiednich procedur niszczenia danych, a także zlecaniu niszczenia ich, wyspecjalizowanym podmiotom zewnętrznym, gwarantującym bezpieczeństwo procesu niszczenia danych odpowiednie do rodzaju nośnika tych danych.
2. Niszczenie zbędnych danych osobowych i/lub ich zbiorów polegać powinno w szczególności na trwałym, fizycznym zniszczeniu nośników danych osobowych i/lub ich zbiorów w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod.
3. Osoby przetwarzające dane osobowe u Właściciela mają obowiązek stosowania oddanych im do dyspozycji narzędzi i technik niszczenia zbędnych danych osobowych i/lub ich zbiorów.

C. BUDYNKI, POMIESZCZENIA I CZĘŚCI POMIESZCZEŃ, TWORZĄCE OBSZAR, W KTÓRYM PRZETWARZANE SA DANE OSOBOWE

§ 9.

1. Właściciel wyznacza budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe. Wykaz budynków stanowi załącznik nr 4 do Polityki bezpieczeństwa.
2. W przypadku, gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część, w której są przetwarzane dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej.
3. Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe może być w szczególności dokonane poprzez montaż barierek, lad lub odpowiednie ustawienie mebli biurowych uniemożliwiające lub co najmniej ograniczające

niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.

4. Pod szczególną ochroną przed niepowołanym dostępem do danych osobowych pozostają urządzenia wchodzące w skład systemu informatycznego. W szczególności stacje robocze (poszczególne komputery) wchodzące w skład tego systemu, powinny być umiejscawiane w sposób uniemożliwiający osobom nieuprawnionym, bezpośredni i niekontrolowany dostęp do ekranów oraz urządzeń służących do przetwarzania, a zwłaszcza kopiowania danych.
5. Osoby nieupoważnione do przetwarzania danych osobowych określonej kategorii, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności nie mające związku z dostępem do tych danych mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar firmy, w którym przetwarzane są dane osobowe – wyłącznie w obecności upoważnionego przedstawiciela Właściciela.
6. Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych.
7. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzana danych osobowych obowiązany jest on umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiających dostęp do danych osobowych osobom niepowołanym.
8. Dostęp do budynków i pomieszczeń, w których przetwarzane są dane osobowe, podlega kontroli. Kontrola dostępu polegać może w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. Właściciel może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.

D. ZBIORY DANYCH OSOBOWYCH

§ 10.

1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych stanowi załącznik nr 5 do Polityki

bezpieczeństwa.

2. Właściciel zabrania tworzenia zbiorów danych osobowych, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych innych niż niezbędne dla realizacji działalności firmy.

E. OPIS STRUKTURY BAZY DANYCH

F. SPOSÓB PRZEPŁYWU DANYCH MIĘDZY ZBIORAMI

G. ZAŁĄCZNIKI

Integralnymi częściami Polityki bezpieczeństwa są:

1. wzór upoważnienia do dostępu do danych osobowych (załącznik nr 1)
2. wzór upoważnienia do przetwarzania danych osobowych (załącznik 2)
3. wykaz osób upoważnionych do przetwarzania danych osobowych (załącznik 3)
4. wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane (załącznik 4)
5. wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych (załącznik 5)
6. ewidencja osób upoważnionych do przetwarzania danych osobowych (załącznik 6)
7. obowiązki administratora danych osobowych (załącznik nr 7)
8. wzór oświadczenia osoby upoważnionej do przetwarzania danych osobowych (załącznik 8)