Polityka bezpieczeństwa

§1

Wprowadzenie oraz uwagi ogólne

1. Polityka Bezpieczeństwa opisuje zasady ochrony danych osobowych gromadzonych i przetwarzanych przez Paulinę Michalik – Stojak Grupę Pierlex z siedzibą w Krakowie, ul. Przy Rondzie 55/2, 31-547 Kraków, legitymującą się numerem NIP 6792995710 , zwaną też w dalszej części niniejszej Polityki „Przedsiębiorcą"

2. Ponieważ działalność Pauliny Michalik – Stojak Grupa Pierlex prowadzona jest w formie jednoosobowej działalności gospodarczej celem Polityki Bezpieczeństwa jest ustanowienie reguł, które należy stosować w działalności Administratora, aby właściwie zabezpieczyć dane osobowe, w szczególności uniknąć:
   a) skarg klientów Administratora w kwestiach ochrony danych osobowych;
   b) udostępnienia danych osobom nieupoważnionym;
   c) zabrania danych przez osobę nieuprawnioną;
   d) przetwarzania danych w sposób sprzeczny z RODO;
   e) nieuprawnionej zmiany, uszkodzenia lub zniszczenia danych.

3. Polityka Bezpieczeństwa stanowi kompleksową całość, a żadna z jej części nie powinna być interpretowana w oderwaniu od pozostałych.

4. Polityka Bezpieczeństwa jest dokumentem wewnętrznym Przedsiębiorcy i nie może być w jakikolwiek sposób oraz w jakiejkolwiek formie udostępniana osobom trzecim. Jest informacją o charakterze poufnym i stanowi tajemnicę przedsiębiorstwami.

5. Przedsiębiorca zapoznaje osoby mające dostęp do danych osobowych z Polityką Bezpieczeństwa oraz dba o systematyczną aktualizację wiedzy tych osób w dziedzinie ochrony danych osobowych.

6. Przedsiębiorca samodzielnie wykonuje wszelkie obowiązki związane z ochroną danych osobowych. Nie powołano Inspektora Ochrony Danych Osobowych (tzw. IODO).

§2

Definicje

Ilekroć w Polityce (zdefiniowanej poniżej) jest mowa o :

1. **Administratorze** – oznacza on Paulinę Michalik – Stojak Grupa Pierlex z siedzibą w Krakowie, ul. Przy Rondzie 55/2, 31-547 Kraków, legitymującą się numerem NIP 6792995710

2. **danych osobowych** – oznacza wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie,
3. **Procesorze** – oznacza podmiot, któremu Administrator powierzył w jakimś zakresie przetwarzanie danych osobowych na podstawie odrębnej umowy, a przetwarzanie wiąże się z inna usługą, którą procesor świadczy dla Administratora.

§ 3

Stosowanie

1. Do zapoznania się i stosowania zasad bezpieczeństwa przetwarzania danych osobowych określonych w Polityce zobowiązani są wszyscy pracownicy Przedsiębiorstwa, osoby zatrudniane przez Przedsiębiorcę, osoby, które wykonują na jego rzecz określone zlecenia stałe bądź jednorazowe, dla wykonania których niezbędne jest udostępnienie przez Przedsiębiorcę danych osobowych.
2. Zasady określone w Polityce stosuje się zarówno do danych osobowych przetwarzanych w formie elektronicznej , jak i danych udostępnionych Przedsiębiorcy przez klientów w jakiejkolwiek innej formie.

§ 4

Administrator Ochrony Danych Osobowych

1. Nadzór nad przetwarzaniem danych osobowych sprawuje Administrator.
2. Administrator stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych u niego danych osobowych odpowiednią do kategorii i zagrożeń danych objętych ochroną, w szczególności Administrator zabezpieczy przetwarzane dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

i. W celu realizacji obowiązku określonego w ust. 2 powyżej odnośnie danych osobowych powierzonych do przetwarzania Administrator prowadzi „Ewidencję Upoważnień i Osób Upoważnionych" stanowiącą załącznik numer 1 do Polityki, jak również „Ewidencję umów powierzenia" stanowiącą załącznik numer 2 do Polityki. Okresowo Administrator wykonuje kontrolę podmiotów którym powierzył przetwarzanie danych osobowych, w zakresie zgodności przetwarzania powierzonych danych z prawem.

3. Ponadto do zadań Administratora należy:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o RODO,
b) prowadzenie rejestru przetwarzania danych osobowych,
c) dokonywanie oceny skutków planowanych operacji przetwarzania danych przed rozpoczęciem ich przetwarzania,
d) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami RODO,
e) zgłaszanie naruszenia ochrony danych osobowych do organu nadzorczego oraz zawiadamiania o tym osoby, której dane te dotyczą,
f) prowadzenie postępowania w przypadku incydentu lub zagrożenia ujawnienia danych osobowych,

a) prowadzenie jawnego rejestru zbiorów danych przetwarzanych przez administratora danych,

§5

Osoby Upoważnione

1. Zgodnie z RODO do danych osobowych uzyskują wyłącznie osoby upoważnione.
2. Upoważnienia do przetwarzania danych osobowych są nadawane w związku z wykonywaniem przez osobę upoważnioną obowiązków lub zadań związanych z przetwarzaniem danych osobowych.
3. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia.
4. „Ewidencję Upoważnień i Osób Upoważnionych" stanowi załącznik numer 1 do Polityki.

§6

Powierzanie

1. Administrator może powierzyć przetwarzanie danych osobowych innemu podmiotowi (Procesor) na podstawie umowy zawartej na piśmie lub w formie elektronicznej.
2. Podmiot, któremu Administrator powierzy przetwarzanie danych osobowych może przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w umowie o powierzeniu.
3. Powierzenie przetwarzania danych osobowych nastąpi po uprzednim zweryfikowaniu przez Administratora środków zabezpieczających powierzane dane osobowe stosowanych przez Procesora.

§ 7

Wykaz budynków

1. Przetwarzanie danych osobowych, w szczególności ich zbieranie, utrwalanie, przechowywanie, opracowywanie lub zmienianie w ramach prowadzenia działalności gospodarczej odbywa się w siedzibie Przedsiębiorcy.
2. Administrator nie udostępnia zbiorów danych osobowych, które znajdują się w jego posiadaniu podmiotom trzecim, nieposiadającym odpowiedniego upoważnienia.

§8

Rejestr czynności przetwarzania

Rejestr czynności przetwarzania danych osobowych prowadzony zgodnie z art. 30 RODO został zamieszczony w załączniku nr 3 .

§ 9

Analiza zagrożeń i opis naruszeń

1. Zagrożenie lub naruszenie bezpieczeństwa przetwarzania danych osobowych stanowią:

a) nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe,

b) ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe;

c) nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,

d) utrata nośnika zawierającego dane osobowe,

e) klęska żywiołowa, w wyniku której utracono poufność danych osobowych,

f) nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym,

g) udostępnianie danych osobowych osobom nieupoważnionym,

h) wejście w posiadanie danych osobowych przez osobę nieuprawnioną,

i) pokonanie zabezpieczeń fizycznych lub programowych,

j) niekontrolowana obecność osób nieuprawnionych w obszarze przetwarzania danych osobowych,

k) niedyskrecja osób uprawnionych do przetwarzania danych osobowych,

l) nieuprawnione kopiowanie danych na nośniki informacji (CD, DVD, pendrive, itp.),

m) niekontrolowane wynoszenie poza obszar przetwarzania danych osobowych nośników informacji i komputerów przenośnych,

n) naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych,

o) podsłuch lub podgląd danych osobowych,

p) elektromagnetyczna emisja ujawniająca,

r) podsłuch akustyczny i podsłuch emisji ujawniającego promieniowania elektromagnetycznego,

s) stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników firmy,

t) zagubienie dokumentów lub utrata przetwarzanych informacji.

§ 10

Określenie środków technicznych i organizacyjnych

niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Administrator celem zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych stosuje następujące środki techniczne i organizacyjne: […]

§ 11

Procedury nadawania i rejestrowania uprawnień w systemie informatycznym

1. W odniesieniu do osób upoważnionych Administrator nadaje identyfikatory użytkownika oraz hasła.
2. Identyfikator użytkownika, który utracił uprawnienia nie może zostać przydzielony innej osobie.
3. System informatyczny posiada mechanizmy umożliwiające określenie uprawnień użytkownika do korzystania z przetwarzanych informacji. Uprawnienia nadawane są w stosownym zakresie każdemu użytkownikowi odpowiednio do jego obowiązków pracowniczych.

§12

Stosowane metody i środki uwierzytelnienia

oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Środkiem uwierzytelnienia dostępu do systemu informatycznego jest identyfikator i hasło nadane przez Administratora. Hasło jest przekazywane użytkownikowi drogą ustną.
2. Hasło składa się z 7 cyfr, liter dużych lub małych oraz jednego znaku specjalnego.
3. Użytkownik jest zobowiązany do zmiany hasła raz do roku.
4. Użytkownik jest zobowiązany do zapewnienia poufności hasła w okresie używania, jak i po jego zakończeniu.
5. Jeżeli dojdzie do ujawnienia hasła użytkownik jest zobowiązany do jego niezwłocznej zmiany oraz zgłoszenia tego faktu Administratorowi.

§ 13

Procedury rozpoczęcia, zawieszenia i zakończenia pracy

1. Użytkownik jest zobowiązany dokonać kontroli poprawności funkcjonowania urządzenia oraz systemu informatycznego na swoim stanowisku pracy przed rozpoczęciem pracy.

2. W razie stwierdzenia nieprawidłowości (w szczególności naruszenia lub zagrażania, o których mowa w Polityce) użytkownik zawiadomi niezwłocznie o tym Administratora.
3. Użytkownik uzyskuje dostęp do systemu informatycznego po wprowadzeniu identyfikatora użytkownika i hasła.
4. Monitory urządzeń służących do przetwarzania danych osobowych należy ustawić w sposób uniemożliwiający wgląd w dane osobowe innych osób – nieupoważnionych do takiego wglądu.
5. W przypadku opuszczenia stanowiska pracy użytkownik jest zobowiązany wylogować się z systemu informatycznego.
6. Po okresie 20 minut bezczynności zostanie uruchomiony wygaszacz ekranu. W celu kontynuowania pracy konieczne będzie ponowne wprowadzenie do systemu informatycznego identyfikatora użytkownika oraz hasła.
7. Po zakończeniu przetwarzania danych w systemie informatycznym użytkownik jest zobowiązany do:

a) wylogowania się z systemu informatycznego,
b) wyłączenia systemu informatycznego
c) wyłączenia urządzenia służącego do przetwarzania danych osobowych (np. komputera).

§ 14

Procedury tworzenia kopii zapasowych zbiorów danych,

programów i narzędzi programowych służących do ich przetwarzania

1. W celu uniknięcia utraty danych osobowych system informatyczny został zabezpieczony przed awarią lub zakłóceniami zasilania.
2. Administrator wykonuje w trybie ciągłym kopie danych z systemu informatycznego. Kopie zapasowe przechowywane są w innej lokalizacji niż serwery i urządzenia główne.

§ 15

Sposób zabezpieczenia systemu informatycznego

przed działalnością szkodliwego oprogramowania

1. Administrator jest zobowiązany do zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania.
2. System informatyczny jest kontrolowany przez Administratora.
3. Źródło szkodliwego oprogramowania mogą stanowić: […]
4. W celu zabezpieczenia systemu informatycznego przed szkodliwym oprogramowaniem zainstalowano następujące oprogramowanie: […]
5. Użytkownikom zabrania się na urządzeniach stanowiących element systemu informatycznego: […]

6. W przypadku pojawienia się na urządzeniu stanowiącym element systemu informatycznego komunikatu o wykryciu zagrożenia użytkownik jest zobowiązany do niezwłocznego poinformowania Administratora.
7. Wykryte zagrożenia są niezwłocznie eliminowane po uprzednim zabezpieczeniu zbioru danych.

§ 16

Procedury odnotowania informacji o przetwarzaniu danych osobowych

1. System informatyczny odnotowuje dla każdej osoby, której dane są w nim przetwarzane, następujące informacje: imię i nazwisko, numer telefonu oraz adres poczty e-mail.
2. Informacje, o których mowa w ust. 1 niniejszego paragrafu są odnotowywane w sposób automatyczny.

§ 17

Raport o danych osobowych

System informatyczny zapewnia możliwość sporządzenia i wydrukowania raportu dla każdej osoby, której dane są przetwarzane w systemie informatycznym, zawierającego informacje, jakie dane o tej osobie są przetwarzane.

§ 18

Procedury przeglądu i konserwacji systemu informatycznego

oraz nośników informacji służących do przetwarzania danych osobowych

1. Za dokonywania przeglądów konserwacji i naprawy systemu informatycznego oraz nośników służących do przetwarzania danych osobowych odpowiedzialny jest Administrator.
2. Administrator dokonuje napraw systemu informatycznego oraz nośników informacji służących do przetwarzania danych osobowych w zależności od potrzeb w celu zapewnienia ciągłości funkcjonowania systemu informatycznego.
3. W przypadku konieczności zlecenia tych czynności podmiotowi zewnętrznemu, osoba ta dokonuje konserwacji lub naprawy pod nadzorem odpowiednio Administratora lub osoby przez niego upoważnionej.
4. Przegląd, konserwacja oraz naprawa powinny zostać wykonane w pomieszczeniach stanowiących obszar, w którym są przetwarzane dane osobowe zgodnie z Polityką, chyba, że przegląd, konserwacja lub naprawa wymaga wyniesienia ich poza obszar.
5. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
6. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do przekazania podmiotowi nieuprawnionemu pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.

7. Administrator prowadzi dokumentację potwierdzającą wykonanie napraw, przeglądów i konserwacji oraz monitoruje ich efekty.
8. Przeglądy i konserwacje systemu informatycznego są dokonywane raz na sześć miesięcy.

§ 19

Korzystanie z komputerów przenośnych

1. Osoba użytkująca komputer przenośny zobowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania komputera poza obszarem przeznaczonym do przetwarzania danych osobowych zgodnie z Polityką.
2. W celu zabezpieczenia komputera przenośnego przed nieuprawnionym dostępem osoba użytkująca komputer przenośny stosuje środki ochrony w postaci szyfrowanego dostępu do komputera oraz szyfrowanego dostępu do plików, w których przechowywane są dane osobowe.
3. Na komputerach przenośnych zastosowano szyfrowanie dysków.

§ 20

Postępowanie w przypadku naruszenia danych osobowych

1. Każda osoba zobowiązana do stosowania Polityki, która stwierdzi zagrożenie lub naruszenie ochrony danych osobowych jest zobowiązana niezwłocznie zgłosić zaistniałe zagrożenie lub naruszenie Administratorowi danych.
2. Administrator przeprowadzi postępowanie wyjaśniające odnośnie naruszenia lub zagrożenia, w szczególności ustali następujące okoliczności:

a) datę stwierdzenia naruszenia lub zagrożenia,
b) przyczyny naruszenia lub zagrożenia,
c) opis zdarzenia,
d) opis stanu technicznego sprzętu.

3. W razie konieczności Administrator zabezpieczy dowody i powiadomi właściwe organy.
4. W ramach postępowania wyjaśniającego, o którym mowa w ust. 2 powyżej Administrator określi:

a) rozmiar zniszczeń,
b) dane do których uzyskano nieuprawniony dostęp lub uległy nieautoryzowanemu zniszczeniu lub modyfikacji,
c) środki naprawcze i zabezpieczające, jakie należy wdrożyć w celu usunięcia skutków zagrożenia lub naruszenia, jak również aby nie dopuścić do zaistnienia zagrożenia lub naruszenia w przyszłości.

5. Administrator sporządzi raport z przeprowadzonego postępowania wyjaśniającego.
6. Administrator niezwłocznie wdroży środki naprawcze i zabezpieczające, o których mowa w ust. 4 c) niniejszego paragrafu.

7. Osoba zobowiązana do powiadomienia Administratora o potencjalnym lub zaistniałym zagrożeniu lub zobowiązaniu, która zaniecha tego obowiązku może podlegać odpowiedzialności karnej.

§ 22

Postanowienia końcowe

Polityka wchodzi w życie z dniem 25.05.2018 roku.