POLITYKA BEZPIECZEŃSTWA INFORMACJI

w

Firmie Handlowo-Usługowej "MAJK" S.C.
ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ
ul. Lubelska 6
27-600 Sandomierz

Niniejsza Polityka Bezpieczeństwa, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).

Definicje:

1. **Administrator Danych Osobowych** – wspólnicy spółki cywilnej - Firma Handlowo-Usługowa "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ, ul. Lubelska 6
27-600 Sandomierz

2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej

3. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych

4. **Użytkownik**– osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych

5. **Zbiór danych**– każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów

6. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych

7. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie

8**. Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie

9. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich danych osobowych przetwarzanych w Firmie Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ, niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej.
3. Polityka jest udostępniana do wglądu osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
4. Dla skutecznej realizacji Polityki Administrator Danych Osobowych zapewnia:
    a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
    b) kontrolę i nadzór nad przetwarzaniem danych osobowych,
    c) monitorowanie zastosowanych środków ochrony.

5. Monitorowanie przez Administratora danych osobowych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
6. Administrator danych osobowych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.
7. Administrator Danych Osobowych (ADO):

a) formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
b) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych;

c) odpowiada za zgodne z prawem przetwarzanie danych osobowych w Firmie Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ
d) zapewnia, aby dane były merytorycznie poprawne i adekwatne w stosunku do celów w jakich są przetwarzane;
e) prowadzi rejestr czynności przetwarzania danych osobowych – Załącznik nr 2 do niniejszej Polityki;
f)
g) udostępnia rejestr czynności przetwarzania danych osobowych do wglądu, każdemu zainteresowanemu w swojej siedzibie;
h) wydaje upoważnienia do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa Załącznik nr 4 do niniejszej Polityki,
i) prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych – Wzór rejestru osób upoważnionych oraz mobilnych nośników Danych określa Załącznik nr 3 do niniejszej Polityki;
j) zapewnia zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

II. Dane osobowe przetwarzane u Administratora Danych Osobowych

1. Administrator Danych Osobowych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator Danych Osobowych wykona czynności określone w art. 35 i nast. RODO.
2. W przypadku planowania nowych czynności przetwarzania Administrator Danych Osobowych dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.

III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa.
2. Wszystkie dane osobowe w Firmie Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
    a) w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych;
    b) dane przetwarzane są rzetelnie i w sposób przejrzysty;
    c) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
    d) dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych;
    e) dane osobowe są prawidłowe i w razie potrzeby uaktualniane;
    f) czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane;
    g) wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO, wzór klauzuli informacji określa Załącznik nr 6 do niniejszej Polityki;
    h) dane są zabezpieczone przed naruszeniami zasad ich ochrony;

3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności:
    a) naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
    b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
    c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
    d) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    e) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;

f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych;
g) naruszenie praw osób, których dane są przetwarzane.

4. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych Osobowych.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są dane osobowe Firmy Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ obejmuje wydzielone pomieszczenia zlokalizowane w siedzibie Spółki, tj. w Sandomierzu (27-600), ul. Lubelska 6.
2. Ponadto, obszarem w którym przetwarzane są dane osobowe, stanowią nośniki danych znajdujące się poza obszarem wskazanym powyżej.

VI. Analiza ryzyka związanego z przetwarzaniem danych osobowych

Możliwe zagrożenia

W przypadku danych przetwarzanych w sposób tradycyjny możemy wyróżnić następujące zagrożenia:

- Oszustwo
- Kradzież
- Sabotaż
- Zdarzenia losowe (np. powódź, pożar)

- Zaniedbania pracowników (niedyskrecja, udostępnienie danych osobie nieupoważnionej)
- Niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania
- Pokonanie zabezpieczeń fizycznych
- Podsłuchy, podglądy
- Brak rejestrowania udostępniania danych
- Niewłaściwe miejsce i sposób przechowywania dokumentacji

1. W przypadku danych przetwarzanych w systemach informatycznych możemy wyróżnić następujące zagrożenia:

- Nieprzydzielenie użytkownikom systemu informatycznego identyfikatorów
- Niewłaściwa administracja systemem
- Niewłaściwa konfiguracja systemu
- Zniszczenie (sfałszowanie) kont użytkowników
- Kradzież danych kont
- Pokonanie zabezpieczeń programowych
- Zaniedbania pracowników (niedyskrecja, udostępnienie danych osobie nieupoważnionej)
- Niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania
- Zdarzenia losowe (np. powódź, pożar)
- Niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania za pomocą nośników informacji i komputerów przenośnych
- Naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione
- Przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci
- Przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych
- Brak rejestrowania zdarzeń tworzenia lub modyfikowania danych.

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych Osobowych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych. Środki te obejmują:

a) ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, nieupoważnione osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie Administratora Danych.
b) zamykanie drzwi do pomieszczeń w których przechowywane są dane osobowe w obszarze przetwarzania danych osobowych określonym w pkt. IV powyżej, na czas nieobecności, w sposób uniemożliwiający dostęp do nich osób trzecich. Obszar przetwarzania będący siedzibą firmy, jest zabezpieczony poprzez antywłamaniowe drzwi oraz wejście z kodem dostępu, uniemożliwiający dostęp do pomieszczeń osobom trzecim. Ponadto każdy upoważniony pracownik pobiera klucz do siedziby z portierni.
c) zamykanie szaf w których przechowywane są dane osobowe w obszarze przetwarzania danych osobowych określonym w pkt. IV powyżej, na czas nieobecności Administratora danych i upoważnionych pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
d) wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.
e) ochronę sprzętu komputerowego wykorzystywanego u Administratora Danych przed złośliwym oprogramowaniem.
f) zabezpieczenie dostępu do urządzeń przy pomocy haseł dostępu.
g) wykorzystanie szyfrowania danych przy ich transmisji.

Szczegółowe wytyczne w zakresie przetwarzania Danych Osobowych przez Osoby Upoważnione zawiera Załącznik nr 1 do niniejszej Polityki.

Określenie wielkości ryzyka

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

VII. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator Danych Osobowych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych Osobowych zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa załącznik nr 8 do niniejszej polityki.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator Danych Osobowych zawiadamia o incydencie także osobę, której dane dotyczą.

VIII. Powierzenie przetwarzania danych osobowych

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.
2. Przed powierzeniem przetwarzania danych osobowych Administrator Danych Osobowych w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.
3. Wzór umowy powierzenia danych osobowych określa Załącznik nr 7 do Polityki Bezpieczeństwa;

IX. Przekazywanie danych do państwa trzeciego

1. Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

X. Postanowienia końcowe

1. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące załączniki.

Załączniki:

Załącznik nr 1
Procedura RODO przetwarzania Danych Osobowych przez Osoby Upoważnione

Załącznik nr 2
Rejestr czynności przetwarzania Danych Osobowych

Załącznik nr 3
Wzór rejestru osób upoważnionych oraz mobilnych nośników Danych

Załącznik nr 4
Wzór upoważnienia do przetwarzania Danych Osobowych

Załącznik nr 5
Wzór oświadczenia potwierdzenia znajomości zasad bezpieczeństwa

Załącznik nr 6
Wzór klauzuli informacyjnej

Załącznik nr 7
Wzór umowy powierzenia przetwarzania danych

Załącznik nr 8

Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego

Załącznik nr 9

Klauzula informacyjna dla kandydatów do pracy

Załącznik nr 10

Klauzula informacyjna dla pracowników