

Polityka Bezpieczeństwa w zakresie przetwarzania danych osobowych

Niniejsza Polityka Bezpieczeństwa, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są w firmie MW LUBSERWIS Wojciech Wojnar 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** – MW LUBSERWIS Wojciech Wojnar, zwana dalej MW LUBSERWIS
- 2.Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
- 3.System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur informatycznych zastosowanych w celu przetwarzania danych
- 4.Zbiór danych osobowych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów
- 5.Przetwarzanie danych** – jakiegokolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych

I. Postanowienia ogólne

- 1.Polityka dotyczy wszystkich Danych osobowych przetwarzanych w firmie MW LUBSERWIS 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. Administrator danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.
2. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób.
- 3.Wszystkie dane osobowe w firmie MW LUBSERWIS 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 osobowe zbierane są w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
 - c) dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych,
 - d) dane są zabezpieczone przed naruszeniami zasad ich ochrony.

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, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w MW LUBSERWIS

2. Administrator danych nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej (art. 14 ust 5 pkt d RODO).

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. Do obowiązków Administratora danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:

- a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków oraz przeszkoleni w zakresie zachowania danych osobowych w firmie, sposobów ich zabezpieczania, w tajemnicy,
- b) pracownicy byli zobowiązani do zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu Administratorowi danych,

- wzór listy upoważnionych pracowników stanowi Załącznik nr 1 Polityki.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe na terenie firmy MW LUBSERWIS obejmuje siedzibę firmy przy ul. Kuźniczej 4 w Ustroniu.

2. Dodatkowo obszar, na którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.

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

1. Administrator danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzania danych.

2. Zastosowane środki ochrony (techniczne i organizacyjne) są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.

Środki obejmują:

- a) ograniczenie dostępu do pomieszczeń, w których przetwarzane są Dane osobowe, jedynie do osób odpowiednio upoważnionych; inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej,
- b) zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt IV powyżej na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
- c) wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów,
- d) wykorzystanie niszczarki lub podobnego urządzenia do skutecznego usuwania dokumentów zawierających dane osobowe,
- e) ochronę sprzętu i sieci komputerowej przed działaniami inicjowanymi z zewnątrz przez złośliwe oprogramowanie bądź wirusy komputerowe,
- f) wykonywanie kopii bezpieczeństwa danych na nośnikach danych,
- g) ochronę sprzętu komputerowego wykorzystywanego u Administratora danych przed złośliwym oprogramowaniem,
- h) zabezpieczenie dostępu do urządzeń, kiedy to możliwe, przy pomocy haseł dostępu,
- i) całodobowy monitoring pomieszczeń firmy prowadzony przez wyspecjalizowaną firmę ochroniarską

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator 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 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 2 do niniejszej Polityki.

3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

VII. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.
2. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące Załączniki:
Załącznik nr 1 – Wzór listy pracowników upoważnionych do Przetwarzania danych osobowych
Załącznik nr 2 - Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Data upoważnienia	Data wygaszenia upoważnienia	Uwagi
1.				
2.				
3.				
4.				
5.				

Raport z naruszenia ochrony danych osobowych nr

Czas wykrycia naruszenia ochrony danych osobowych	Data: _____ Godzina: _____
Miejsce wykrycia naruszenia ochrony danych osobowych	
Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane w naruszenie lub będące jego świadkiem	
Rodzaj naruszenia i okoliczności	
Podjęte działania dokumentujące zaistnienie naruszenia	
Ocena przyczyn wystąpienia naruszenia	
Postępowanie wyjaśniające i naprawcze	

.....
Data.....
Podpis osoby upoważnionej przez
Administratora danych