

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§1

Celem instrukcji jest określenie sposobu postępowania gdy:

1. Stwierdzono naruszenie zabezpieczeń danych osobowych
2. W przypadku danych przetwarzanych w formie tradycyjnej stan pomieszczeń, szaf, okien, drzwi, dokumentów lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.
3. W przypadku danych przetwarzanych w formie elektronicznej stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu, jakość komunikacji lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

§2

Instrukcja określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych, zgodne z „Tabelą form naruszeń bezpieczeństwa danych osobowych”, stanowiącą załącznik A do niniejszej instrukcji.

§3

Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

- a) nieautoryzowany dostęp do danych,
- b) nieautoryzowane modyfikacje lub zniszczenie danych,
- c) udostępnienie danych nieautoryzowanym podmiotom,
- d) nielegalne ujawnienie danych,
- e) pozyskiwanie danych z nielegalnych źródeł.

§4

1. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić ten fakt bezpośrednio przełożonemu, Administratorowi Bezpieczeństwa Informacji, a następnie postępować stosownie do podjętej przez niego decyzji.
2. Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zawierać:
 - a) opisanie symptomów naruszenia zabezpieczeń danych osobowych,
 - b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych,
 - c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
 - d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§5

Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:

- a) minimalizację negatywnych skutków zdarzenia,
- b) wyjaśnienie okoliczności zdarzenia,
- c) zabezpieczenie dowodów zdarzenia,
- d) umożliwienie dalszego bezpiecznego przetwarzania danych.

§6

W celu realizacji zadań wynikających z niniejszej instrukcji Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

- a) żądania wyjaśnień od pracowników,
- b) korzystania z pomocy konsultantów,
- c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§7

Polecenia Administratora Bezpieczeństwa Informacji lub innej upoważnionej przez niego osoby wydawane w celu realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.

§8

Odmowa udzielenia wyjaśnień lub współpracy z Administratorem Bezpieczeństwa Informacji lub inną upoważnioną przez niego osobą traktowana będzie jako naruszenie obowiązków pracowniczych.

§9

Administrator Bezpieczeństwa Informacji po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości. Wzór raportu stanowi załącznik B do niniejszej instrukcji.

§10

Nieprzestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

§11

Jeżeli skutkiem działania określonego w §10 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.

§12

Jeżeli skutkiem działania określonego w §10 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Prawa Cywilnego.