Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych AVSI POLSKA z siedzibą w Warszawie

Rozdział 1

Postanowienia ogólne

§ 1

1. Instrukcja niniejsza określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku gdy:

a) stwierdzono naruszenie zabezpieczenia systemu ochrony danych osobowych w tym systemu informatycznego,

b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych.

2. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie, jest wyznaczony przez administratora danych osobowych – Informatyk.

3. Wszystkie osoby przetwarzające dane osobowe na polecenie administratora danych osobowych zobowiązują się podejmować wszelkie zgodne z prawem środki zaradcze, w tym w szczególności przestrzegać warunków określonych w procedurach ochrony danych osobowych obowiązujących w AVSI POLSKA aby nie dopuścić do naruszenia ochrony danych osobowych.

4. Przez naruszenie ochrony danych osobowych należy rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

5. W przypadku wykrycia naruszenia ochrony danych osobowych, jak również w przypadku próby lub ryzyka takiego naruszenia, osoba przetwarzające dane osobowe jest zobowiązana do natychmiastowego podjęcia

niezbędnych działań zaradczych oraz do zawiadomienia administratora danych osobowych, nie później niż w ciągu godziny od wykrycia naruszenia albo próby lub ryzyka takiego naruszenia.

6. W przypadku naruszenia ochrony danych osobowych, administrator danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

7. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, administrator danych osobowych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o taki naruszeniu, chyba, że zachodzą okoliczności określone w art. 34 ust. 3 i 4 RODO lub w innych przepisach prawa.

8. Administrator danych osobowych prowadzi w formie pisemnej rejestr naruszeń ochrony danych osobowych, w którym szczegółowo opisuje:

a) okoliczności naruszenia ochrony danych osobowych,

b) skutki naruszenia ochrony danych osobowych,

c) podjęte działania zaradcze

Rozdział 2

Tryb i zasady postępowania w przypadku stwierdzenia

naruszenia zabezpieczenia systemu informatycznego

§ 2

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym Informatyka.

2. Informatyk po otrzymaniu powiadomienia:

a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, zmiana haseł),

b) zabezpiecza, utrwala wszelkie informacje i dokumenty, które mogą stanowić pomoc przy ustaleniu przyczyn naruszenia,

c) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,

d) niezwłocznie przywraca prawidłowy stan działania systemu, a w przypadku uszkodzenia baz danych odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,

e) dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,

f) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu (włamaniu do systemu), opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

3. Raport wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) Informatyk przekazuje administratorowi danych osobowych jednostki.
4. Informatyk w porozumieniu z administratorem danych osobowych podejmuje niezbędne działania w celu zapobieżenia naruszeniom zabezpieczeń systemu w przyszłości.

Rozdział 3

Tryb postępowania w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych

§ 3

1. Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych, obowiązana jest niezwłocznie powiadomić o tym Informatyka lub inną upoważnioną przez niego osobę.
2. Informatyk po otrzymaniu powiadomienia (stosownie do przypuszczalnego rodzaju naruszeń):

a) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

b) sprawdza sposób działania programu (w tym również obecność wirusów komputerowych),

c) sprawdza jakość komunikacji w sieci telekomunikacyjnej,

3. W przypadku stwierdzenia naruszenia zabezpieczeń danych:

a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, blokuje dostęp do sieci telekomunikacyjnej, do programów oraz zbiorów danych

itp.),

b) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,

c) niezwłocznie przywraca prawidłowy stan działania systemu,

d) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek ich naruszenia,

e) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

4. Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie), Informatyk przekazuje administratorowi danych osobowych jednostki.

5. Informatyk, w porozumieniu z administratorem danych osobowych, podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

a) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,

b) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, informuje administratora danych osobowych o potrzebie przeprowadzenia dodatkowych kursów i szkoleń osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągniecie konsekwencji prawem przewidzianych.

Rozdział 4

Postanowienia końcowe

§ 4

1. Każda osoba wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych zobowiązana jest do zapoznania się z niniejszą instrukcją. Wykonanie powyższego zobowiązania pracownik potwierdza własnoręcznym podpisem.

2. Wszelkie zmiany niniejszej instrukcji skutkują wobec osób, których dotyczą, z dniem ich doręczenia na piśmie.