Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych

Rozdział 1.

Postanowienia ogólne

§ 1

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

   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,

   2) 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 – inspektor ochrony danych.

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 administratora danych osobowych oraz inspektora ochrony danych.
2. Inspektor ochrony danych po otrzymaniu powiadomienia:

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

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

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

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

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

6) 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) inspektor ochrony danych przekazuje administratorowi danych osobowych jednostki.
4. Inspektor ochrony danych 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 inspektora ochrony danych lub inną upoważnioną przez niego osobę.
2. Inspektor ochrony danych po otrzymaniu powiadomienia (stosownie do przypuszczalnego rodzaju naruszeń):

   1) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

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

   3) sprawdza jakość komunikacji w sieci telekomunikacyjnej,

   4) sprawdza zawartość zbioru danych osobowych,

   5) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.

3. W przypadku stwierdzenia naruszenia zabezpieczeń danych:

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

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

   3) niezwłocznie przywraca prawidłowy stan działania systemu,

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

   5) 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), inspektor ochrony danych przekazuje administratorowi danych osobowych jednostki.

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

   1) 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,

   2) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia 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.

03.09.2018 r. Monika Cwiżel

Data i podpis inspektora ochrony danych