

## **A. Środki bezpieczeństwa na poziomie podstawowym**

### **I**

1. Obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
2. Przebywanie osób nieuprawnionych w obszarze, o którym mowa w § 4 pkt 1 rozporządzenia, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

### **II**

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
  - a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
  - b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

### **III**

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

- 1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- 2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

### **IV**

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.
3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
4. Kopie zapasowe:
  - a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
  - b) usuwa się niezwłocznie po ustaniu ich użyteczności.

### **V**

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

### **VI**

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- 1) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- 2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- 3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

## **VII**

Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

### **B. Środki bezpieczeństwa na poziomie podwyższonym**

#### **VIII**

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

#### **IX**

Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

#### **X**

Instrukcja zarządzania systemem informatycznym, o której mowa w § 5 rozporządzenia, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika.

#### **XI**

Administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa określone w części A załącznika, o ile zasady zawarte w części B nie stanowią inaczej.

### **C. Środki bezpieczeństwa na poziomie wysokim**

#### **XII**

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
  - a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
  - b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

#### **XIII**

Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

#### **XIV**

Administrator danych stosuje na poziomie wysokim środki bezpieczeństwa, określone w części A i B załącznika, o ile zasady zawarte w części C nie stanowią inaczej.