Dz. U. z 2004 r. Nr 100, poz. 1024

ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 29 kwietnia 2004 r.

w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Na podstawie art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285) zarządza się, co następuje:

§ 1.

Rozporządzenie określa:

1) sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
2) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
3) wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

§ 2.

Ilekroć w rozporządzeniu jest mowa o:

1) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";
2) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
3) haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
4) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
5) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
6) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
7) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
8) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
9) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
10) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
11) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 3.

1. Na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją".

2. Dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej.

3. Dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

§ 4.

Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

4) sposób przepływu danych pomiędzy poszczególnymi systemami;

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 5.

Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

5) sposób, miejsce i okres przechowywania:

a) elektronicznych nośników informacji zawierających dane osobowe,

b) kopii zapasowych, o których mowa w pkt 4,

6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;

7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;

8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§ 6.

1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:

   1) podstawowy;

   2) podwyższony;

   3) wysoki.

2. Poziom co najmniej podstawowy stosuje się, gdy:

   1) w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 27 ustawy, oraz

   2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie

jest połączone z siecią publiczną.

3. Poziom co najmniej podwyższony stosuje się, gdy:

   1) w systemie informatycznym przetwarzane są dane osobowe, o których mowa w art. 27 ustawy, oraz

   2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

4. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

5. Opis środków bezpieczeństwa stosowany na poziomach, o których mowa w ust. 1, określa załącznik do rozporządzenia.

§ 7.

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

   1) daty pierwszego wprowadzenia danych do systemu;

   2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

   3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;

   4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

   5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 8.

System informatyczny służący do przetwarzania danych, który został dopuszczony przez właściwą służbę ochrony państwa do przetwarzania informacji niejawnych, po uzyskaniu certyfikatu wydanego na podstawie przepisów ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) spełnia wymogi niniejszego rozporządzenia pod względem bezpieczeństwa na poziomie wysokim.

§ 9.

Administrator przetwarzanych w dniu wejścia w życie niniejszego rozporządzenia danych osobowych jest obowiązany dostosować systemy informatyczne służące do przetwarzania tych danych do wymogów określonych w § 7 oraz w załączniku do rozporządzenia w terminie 6 miesięcy od dnia wejścia w życie niniejszego rozporządzenia.

§ 10.

Rozporządzenie wchodzi w życie z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej.

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024)

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.