Dz. U. z 1998 r. Nr 80, poz. 521

ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI
z dnia 3 czerwca 1998 r.

w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Na podstawie art. 45 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883) zarządza się, co następuje:

§ 1

Ilekroć w rozporządzeniu jest mowa o:
1) systemie informatycznym - należy przez to rozumieć system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje,
2) zabezpieczeniu systemu informatycznego - należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

§ 2

W celu właściwego zarządzania zabezpieczeniami systemu informatycznego oraz dla ochrony danych osobowych w nim przetwarzanych, administrator danych, przed przystąpieniem do przetwarzania danych osobowych, jest obowiązany:
1) określić cele, strategię i politykę zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
2) zidentyfikować i przeanalizować zagrożenia i ryzyko, na które może być narażone przetwarzanie danych osobowych,
3) określić potrzeby w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych, z uwzględnieniem potrzeby kryptograficznej ochrony danych osobowych, w szczególności podczas ich przesyłania za pomocą urządzeń teletransmisji danych,
4) określić zabezpieczenia adekwatne do zagrożeń i ryzyka,
5) monitorować działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych i ich przetwarzania,
6) opracować i wdrożyć program szkolenia w zakresie zabezpieczeń systemu informatycznego,
7) wykrywać i właściwie reagować na przypadki naruszenia bezpieczeństwa danych osobowych i systemów informatycznych je przetwarzających.

§ 3

Administrator danych wyznacza osobę, zwaną dalej *„administratorem bezpieczeństwa informacji”*, 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 zabezpieczeń.

§ 4

Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę tych danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem - w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

§ 5

Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych.

§ 6

1. Administrator danych jest obowiązany do opracowania instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.
2. Instrukcja, o której mowa w ust. 1, określa tryb postępowania 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 tych danych.
3. W przypadkach, o których mowa w ust. 2, osoba przetwarzająca dane osobowe jest obowiązana niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji lub inną upoważnioną przez niego osobę.

§ 7

1. Administrator danych określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
2. Przebywanie wewnątrz obszaru, o którym mowa w ust. 1, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą administratora danych lub osoby przez niego upoważnionej.
3. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 8

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

§ 9

Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem, o którym mowa w § 7 ust. 1, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a w szczególności powinna:
1) zabezpieczyć dostęp do komputera hasłem,

2) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych.

§ 10

1. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
3. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
4. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 11

1. Administrator danych jest obowiązany do opracowania instrukcji, określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
2. Instrukcja, o której mowa w ust. 1, powinna zawierać w szczególności:
   1) określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności,
   2) określenie sposobu rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności,
   3) procedury rozpoczęcia i zakończenia pracy,
   4) metodę i częstotliwość tworzenia kopii awaryjnych,
   5) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,
   6) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,
   7) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
   8) sposób postępowania w zakresie komunikacji w sieci komputerowej.

§ 12

1. Kopie awaryjne, o których mowa w § 11 ust. 2 pkt 4, nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
2. Kopie awaryjne należy:
   1) okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu,
   2) bezzwłocznie usuwać po ustaniu ich użyteczności.

§ 13

Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.

§ 14

1. System informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych.
2. Administrator bezpieczeństwa informacji jest odpowiedzialny za właściwy nadzór nad funkcjonowaniem mechanizmów, o których mowa w ust. 1.
3. Dla każdego użytkownika systemu informatycznego, w którym przetwarza się dane osobowe, administrator danych lub upoważniona przez niego osoba ustala odrębny identyfikator i hasło.
4. Identyfikator, o którym mowa w ust. 1, wpisuje się do ewidencji określonej w art. 39 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883), zwanej dalej *„ustawą”*, wraz z imieniem i nazwiskiem użytkownika, oraz rejestruje w systemie informatycznym.
5. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
6. Hasło użytkownika powinno być zmieniane, co najmniej raz na miesiąc.
7. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
8. Hasła użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy, również po upływie ich ważności.
9. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

§ 15

1. Jeżeli istnieją odpowiednie możliwości techniczne, ekrany monitorów stanowisk dostępu do danych osobowych powinny być automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.
2. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

§ 16

Dla każdej osoby, której dane są przetwarzane w systemie informatycznym, system ten powinien zapewniać odnotowanie:

1) daty pierwszego wprowadzenia danych tej osoby,
2) źródła pochodzenia danych, jeśli dane pochodzić mogą z różnych źródeł,
3) identyfikatora użytkownika wprowadzającego dane,
4) informacji, komu, kiedy i w jakim zakresie dane zostały udostępnione, jeśli przewidziane jest udostępnianie danych innym podmiotom, chyba, że dane te traktuje się jako dane powszechnie dostępne,
5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 7 ustawy, po jego uwzględnieniu, oraz sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy.

§ 17

System informatyczny służący do przetwarzania danych osobowych powinien umożliwić udostępnienie na piśmie, w powszechnie zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, wraz z informacjami, o których mowa w § 16.

§ 18

Administrator danych przetwarzanych w zbiorze istniejącym w dniu wejścia w życie rozporządzenia obowiązany jest do wykonania czynności, o których mowa w § 2, w terminie trzech miesięcy od dnia wejścia w życie rozporządzenia.

§ 19

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.