644

ROZPORZĄDZENIE MINISTRA SPRAWIEDLIWOŚCI

z dnia 11 czerwca 2001 r.

w sprawie gromadzenia danych osobowych w Krajowym Rejestrze Karnym oraz usuwania tych danych z Rejestru.

Na podstawie art. 17 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. Nr 50, poz. 580 i z 2001 r. Nr 56, poz. 579) zarządza się, co następuje:

§ 1. Rozporządzenie określa szczegółowe zasady, sposób, tryb oraz warunki techniczne i organizacyjne gromadzenia danych osobowych w Krajowym Rejestrze Karnym oraz usuwania tych danych z Rejestru.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) ustawa — ustawę z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym,

2) Rejestr — Krajowy Rejestr Karny.

§ 3. Do zabezpieczenia danych osobowych zgromadzonych w Rejestrze stosuje się przepisy rozporządzenia 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 (Dz. U. Nr 80, poz. 521), ze zmianami i uzupełnieniami wynikającymi z niniejszego rozporządzenia.

§ 4. W celu zabezpieczenia danych osobowych zgromadzonych w Rejestrze dyrektor Biura Informacyjnego Rejestru Karnego, zwany dalej „dyrektorem":

1) identyfikuje i analizuje zagrożenia i ryzyko, na które może być narażone przetwarzanie danych osobowych,

2) określa potrzeby w zakresie zabezpieczenia kartotek i systemu informatycznego,

3) określa zabezpieczenia danych osobowych adekwentne do zagrożeń i ryzyka,

4) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych i ich przetwarzania,

5) opracowuje i wdraża program szkolenia w zakresie zabezpieczeń kartotek i systemu informatycznego,

6) wykrywa i reaguje na przypadki naruszenia bezpieczeństwa danych osobowych zgromadzonych w kartotekach i systemie informatycznym.

§ 5. Osobą odpowiedzialną za bezpieczeństwo danych osobowych zgromadzonych w kartotekach i systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób nieuprawnionych do kartotek i systemu informatycznego, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemach zabezpieczeń jest administrator bezpieczeństwa informacji, wyznaczony przez dyrektora.

§ 6. 1. Do obsługi kartotek i systemu informatycznego oraz urządzeń wchodzących w jego skład dopuszcza się wyłącznie osoby upoważnione przez dyrektora, zwane dalej „osobami uprawnionymi".

2. Indywidualny zakres czynności osób uprawnionych określa zakres odpowiedzialności za ochronę danych osobowych przed dostępem osób nieuprawnionych, wykorzystywaniem przez osoby nieuprawnione, uszkodzeniem lub zniszczeniem.

§ 7. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każdą osobę uprawnioną zaznajamia się z przepisami dotyczącymi Rejestru i ochrony danych osobowych w nim zgromadzonych.

§ 8. 1. W przypadku naruszenia kartotek lub systemu informatycznego, w których są zgromadzone dane osobowe, osoba uprawniona postępuje w sposób określony przez dyrektora.

2. O każdym przypadku naruszenia kartotek lub systemu informatycznego, w których są zgromadzone dane osobowe, osoba uprawniona jest obowiązana niezwłocznie powiadomić dyrektora oraz administratora bezpieczeństwa informacji.

§ 9. 1. Pomieszczenia lub części pomieszczeń, tworzące obszar, w którym są przetwarzane dane osobowe zgromadzone w kartotekach oraz w bazie danych systemu informatycznego, określa dyrektor.

2. Pomieszczenia lub części pomieszczeń, o których mowa w ust. 1, wyposaża się w zabezpieczenia techniczne uniemożliwiające utratę zbiorów danych osobowych oraz zabezpieczenia chroniące przed dostępem do nich osób nieuprawnionych, wykorzystywaniem przez osoby nieuprawnione, uszkodzeniem lub zniszczeniem oraz zamyka się na czas nieobecności w nich osób uprawnionych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 10. Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą lub zniekształceniem tych danych spowodowanych awarią zasilania lub zakłóceniami w sieci zasilającej.

§ 11. Osoba uprawniona wprowadza do systemu informatycznego dane osobowe zawarte w kartach rejestracyjnych i zawiadomieniach o zmianach ewidencyjnych, a następnie umieszcza je w odpowiedniej kartotece.

§ 12. 1. Karty rejestracyjne oraz zawiadomienia o zmianach ewidencyjnych usuwa się z kartotek poprzez fizyczne zniszczenie przez osoby uprawnione, w sposób uniemożliwiający ustalenie tożsamości osoby, której dane te dotyczą.

2. Zapis informacji dotyczących udostępnienia danych osobowych zgromadzonych w Rejestrze usuwa się z bazy danych systemu informatycznego z chwilą usunięcia wszystkich zgromadzonych tam danych o osobie.

§ 13. 1. Urządzenia lub nośniki informatyczne, zawierające dane osobowe przeznaczone do usunięcia z Rejestru, pozbawia się zapisu tych danych.

2. W przypadku gdy pozbawienie nośników informatycznych zapisu danych osobowych nie jest możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie.

§ 14. Urządzenia lub nośniki informatyczne, zawierające dane osobowe, przeznaczone do naprawy, przed naprawą pozbawia się zapisu tych danych albo naprawia się je pod nadzorem administratora bezpieczeństwa informacji.

§ 15. 1. Osoba uprawniona sporządza kopie awaryjne danych osobowych zgromadzonych w systemie informatycznym Rejestru.

2. Kopie awaryjne należy:

1) okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych osobowych w przypadku awarii systemu,
2) bezzwłocznie usuwać po ustaniu ich użyteczności, w sposób określony w § 13.

3. Kopii awaryjnych nie przechowuje się w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

§ 16. 1. System informatyczny, w którym zgromadzone są dane osobowe, wyposaża się w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do przetwarzanych danych.

2. Dla każdej osoby uprawnionej będącej użytkownikiem systemu informatycznego, o którym mowa w ust. 1, dyrektor lub osoba przez niego upoważniona ustala odrębny identyfikator i hasło użytkownika.

3. Identyfikator, o którym mowa w ust. 2, 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, z 2000 r. Nr 12, poz. 136, Nr 50, poz. 580 i Nr 116, poz. 1216 oraz z 2001 r. Nr 42, poz. 474 i Nr 49, poz. 509) wraz z imieniem i nazwiskiem użytkownika oraz rejestruje w systemie informatycznym.

4. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła użytkownika.

5. Hasło użytkownika zmienia się co najmniej raz na miesiąc.

6. Identyfikatora użytkownika nie zmienia się, a po wyrejestrowaniu użytkownika z systemu informatycznego nie przydziela się innej osobie.

7. Hasła użytkownika nie udostępnia się, również po upływie jego ważności.

8. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło użytkownika oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

9. Identyfikator osoby, o której mowa w ust. 8, wykreśla się z ewidencji z chwilą usunięcia wszystkich danych osobowych wprowadzonych przez tę osobę do kartotek i systemu informatycznego.

§ 17. 1. Ekrany monitorów na stanowiskach dostępu do danych osobowych przetwarzanych w systemie informatycznym są samoczynnie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.

2. W pomieszczeniach, gdzie mogą przebywać osoby postronne, monitory, o których mowa w ust. 1, powinny być ustawione w sposób uniemożliwiający tym osobom wgląd w dane.

§ 18. Dla każdej osoby, której dane osobowe są przetwarzane w Rejestrze, system informatyczny zapewnia odnotowanie:

1) daty wprowadzenia pierwszych i kolejnych danych tej osoby,
2) identyfikatora użytkownika wprowadzającego dane,
3) informacji, jakie dane osobowe zostały wprowadzone do Rejestru,
4) informacji, komu, kiedy, w jakim zakresie i przez kogo zostały udostępnione dane zgromadzone w Rejestrze.

§ 19. Rozporządzenie wchodzi w życie z dniem 22 czerwca 2001 r.

Minister Sprawiedliwości: *L. Kaczyński*