1929

ROZPORZĄDZENIE MINISTRA SPRAWIEDLIWOŚCI

z dnia 7 listopada 2003 r.

w sprawie gromadzenia danych osobowych i danych o podmiotach zbiorowych 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, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa warunki, w tym techniczne i organizacyjne, sposób oraz tryb gromadzenia danych osobowych oraz danych o podmiotach zbiorowych w Krajowym Rejestrze Karnym, zwanym dalej „Rejestrem", oraz usuwania tych danych z Rejestru.

§ 2. 1. 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 oraz z 2001 r. Nr 121, poz. 1306), ze zmianami i uzupełnieniami wynikającymi z niniejszego rozporządzenia.

2. Do zabezpieczenia danych o podmiotach zbiorowych zgromadzonych w Rejestrze stosuje się odpowiednio 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, ze zmianami i uzupełnieniami wynikającymi z niniejszego rozporządzenia.

§ 3. W celu zabezpieczenia danych osobowych oraz danych o podmiotach zbiorowych zgromadzonych w Rejestrze dyrektor Biura Informacyjnego Krajowego Rejestru Karnego, zwany dalej „dyrektorem":

1) identyfikuje i analizuje zagrożenia i ryzyko, na które może być narażone przetwarzanie danych osobowych i danych o podmiotach zbiorowych;
2) określa potrzeby w zakresie zabezpieczenia kartotek i systemu informatycznego;
3) określa sposoby zabezpieczenia danych osobowych i danych o podmiotach zbiorowych adekwatne do zagrożeń i ryzyka;
4) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych oraz danych o podmiotach zbiorowych 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 i danych o podmiotach zbiorowych zgromadzonych w kartotekach i systemie informatycznym.

§ 4. Osobą odpowiedzialną za bezpieczeństwo danych osobowych i danych o podmiotach zbiorowych 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.

§ 5. 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 i danych o podmiotach zbiorowych przed dostępem osób nieuprawnionych, wykorzystywaniem przez osoby nieuprawnione, uszkodzeniem lub zniszczeniem.

§ 6. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych i danych o podmiotach zbiorowych każdą osobę uprawnioną zaznajamia się z przepisami dotyczącymi Rejestru i ochrony danych w nim zgromadzonych, co osoba uprawniona potwierdza własnoręcznym podpisem.

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

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

§ 8. 1. Pomieszczenia lub części pomieszczeń, tworzące obszar, w którym są przetwarzane dane osobowe i dane o podmiotach zbiorowych 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

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 56, poz. 579, z 2002 r. Nr 74, poz. 676 i Nr 197, poz. 1661 oraz z 2003 r. Nr 137, poz. 1302.

osobowych i danych o podmiotach zbiorowych 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.

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

§ 10. Osoba uprawniona wprowadza do systemu informatycznego dane osobowe i dane o podmiotach zbiorowych zawarte w kartach rejestracyjnych i zawiadomieniach o zmianach ewidencyjnych oraz zawiadomieniach dotyczących podmiotów zbiorowych, a następnie umieszcza je w odpowiedniej kartotece.

§ 11. 1. Karty rejestracyjne oraz zawiadomienia o zmianach ewidencyjnych i dotyczące podmiotów zbiorowych usuwa się z kartotek poprzez fizyczne zniszczenie przez osoby uprawnione, w sposób uniemożliwiający ustalenie tożsamości osoby i danych identyfikujących podmiot zbiorowy, których dane te dotyczą.

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

§ 12. 1. Urządzenia lub elektroniczne nośniki informacji, zawierające dane osobowe lub dane o podmiocie zbiorowym, przeznaczone do usunięcia z Rejestru, pozbawia się zapisu tych danych.

2. W przypadku gdy pozbawienie elektronicznych nośników informacji zapisu danych osobowych lub danych o podmiotach zbiorowych nie jest możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie.

§ 13. Urządzenia lub elektroniczne nośniki informacji, zawierające dane osobowe lub dane o podmiotach zbiorowych, przeznaczone do naprawy, przed naprawą pozbawia się zapisu tych danych albo naprawia się je pod nadzorem administratora bezpieczeństwa informacji.

§ 14. 1. Osoba uprawniona sporządza kopie awaryjne danych osobowych lub danych o podmiotach zbiorowych zgromadzonych w systemie informatycznym Rejestru.

2. Kopie awaryjne należy:

1) okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych osobowych lub danych o podmiotach zbiorowych w przypadku awarii systemu;

2) bezzwłocznie usuwać po ustaniu ich użyteczności, w sposób określony w § 12.

3. Kopii awaryjnych nie przechowuje się w tych samych pomieszczeniach, w których są przechowywane zbiory danych osobowych i danych o podmiotach zbiorowych eksploatowanych na bieżąco. Przepis § 8 ust. 2 stosuje się odpowiednio.

§ 15. 1. Systemy informatyczne, w których są zgromadzone dane osobowe i dane o podmiotach zbiorowych, 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. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271) wraz z imieniem i nazwiskiem użytkownika oraz rejestruje w systemie informatycznym.

4. Bezpośredni dostęp do danych osobowych i danych o podmiotach zbiorowych 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 i danych o podmiotach zbiorowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło użytkownika oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

§ 16. 1. Ekrany monitorów na stanowiskach dostępu do danych osobowych i danych o podmiotach zbiorowych 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.

§ 17. Dla każdej osoby i podmiotu zbiorowego, których dane są przetwarzane w Rejestrze, system informatyczny zapewnia spójne odnotowanie:

1) daty wprowadzenia pierwszych i kolejnych danych tej osoby lub podmiotu zbiorowego;

2) identyfikatora użytkownika wprowadzającego dane;

3) informacji, jakie dane osobowe lub dane o podmiocie zbiorowym zostały wprowadzone do Rejestru,

4) informacji komu, kiedy, w jakim zakresie i przez kogo zostały udostępnione dane zgromadzone w Rejestrze.

§ 18. Traci moc rozporządzenie Ministra Sprawiedliwości z dnia 11 czerwca 2001 r. w sprawie gromadzenia danych osobowych w Krajowym Rejestrze Karnym oraz usuwania tych danych z Rejestru (Dz. U. Nr 63, poz. 644).

§ 19. Rozporządzenie wchodzi w życie z dniem 28 listopada 2003 r.

Minister Sprawiedliwości: *G. Kurczuk*