1681

ROZPORZĄDZENIE MINISTRA PRACY I POLITYKI SPOŁECZNEJ[1)]

z dnia 28 listopada 2007 r.

w sprawie warunków, sposobu oraz trybu gromadzenia i usuwania danych w ramach Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności

Na podstawie art. 6d ust. 6 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. Nr 123, poz. 776, z późn. zm.[2)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa szczegółowe warunki, w tym techniczne i organizacyjne, sposób oraz tryb gromadzenia i usuwania danych w ramach Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności, zwanego dalej „systemem".

§ 2. 1. System jest systemem teleinformatycznym budowanym w ramach standardów określonych przepisami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565 oraz z 2006 r. Nr 12, poz. 65 i Nr 73, poz. 501).

2. Dla przetwarzania danych osobowych w systemie ustala się wysoki poziom bezpieczeństwa.

§ 3. 1. Minister właściwy do spraw zabezpieczenia społecznego zapewnia eksploatację systemu.

2. W systemie użytkuje się 17 baz danych, w tym jedna przeznaczona jest dla Pełnomocnika Rządu do Spraw Osób Niepełnosprawnych, zwanego dalej „Pełnomocnikiem", i 16 dla wojewódzkich zespołów do spraw orzekania o niepełnosprawności, zwanych dalej „wojewódzkimi zespołami". Każda baza wojewódzkiego zespołu zawiera wydzielone logicznie bazy powiatowych zespołów do spraw orzekania o niepełnosprawności, zwanych dalej „powiatowymi zespołami".

[1)] Minister Pracy i Polityki Społecznej kieruje działem administracji rządowej — zabezpieczenie społeczne, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 16 listopada 2007 r. w sprawie szczegółowego zakresu działania Ministra Pracy i Polityki Społecznej (Dz. U. Nr 216, poz. 1598).

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1997 r. Nr 160, poz. 1082, z 1998 r. Nr 99, poz. 628, Nr 106, poz. 668, Nr 137, poz. 887, Nr 156, poz. 1019 i Nr 162, poz. 1118 i 1126, z 1999 r. Nr 49, poz. 486, Nr 90, poz. 1001, Nr 95, poz. 1101 i Nr 111, poz. 1280, z 2000 r. Nr 48, poz. 550 i Nr 119, poz. 1249, z 2001 r. Nr 39, poz. 459, Nr 100, poz. 1080, Nr 125, poz. 1368, Nr 129, poz. 1444 i Nr 154, poz. 1792 i 1800, z 2002 r. Nr 169, poz. 1387, Nr 200, poz. 1679 i 1683 i Nr 241, poz. 2074, z 2003 r. Nr 7, poz. 79, Nr 90, poz. 844, Nr 223, poz. 2217 i Nr 228, poz. 2262, z 2004 r. Nr 96, poz. 959, Nr 99, poz. 1001 i Nr 240, poz. 2407, z 2005 r. Nr 44, poz. 422, Nr 132, poz. 1110, Nr 163, poz. 1362, Nr 164, poz. 1366 i Nr 167, poz. 1398, z 2006 r. Nr 63, poz. 440, Nr 94, poz. 651 i Nr 170, poz. 1217 oraz z 2007 r. Nr 23, poz. 144, Nr 115, poz. 791 i Nr 181, poz. 1288.

3. W zakresie funkcjonalności system zapewnia:

1) Pełnomocnikowi — prowadzenie rejestrów szkoleń i kontroli, generowanie sprawozdań, sporządzanie analiz i statystyk, wspomaganie monitoringu procesu orzekania w nadzorowanych przez niego powiatowych i wojewódzkich zespołach i administrowanie systemem;
2) wojewódzkim zespołom — prowadzenie rejestrów odwołań, orzeczeń, członków wojewódzkiego zespołu, wydatków wojewódzkiego zespołu, szkoleń i kontroli oraz generowanie niezbędnych dokumentów wymaganych w procesie orzekania, okresowe generowanie sprawozdań, wspomaganie monitoringu procesu orzekania w powiatowych zespołach;
3) powiatowym zespołom — prowadzenie rejestrów wniosków, orzeczeń, odwołań, członków powiatowego zespołu, wydatków powiatowego zespołu oraz legitymacji, generowanie niezbędnych dokumentów wymaganych w procesie orzekania, okresowe generowanie sprawozdań.

§ 4. 1. System umożliwia nadawanie uprawnień użytkownikom, zgodnie z przydzielonymi im poziomami dostępu, według następujących zasad:

1) poziom I — wprowadzenie danych;
2) poziom II — wprowadzenie danych i możliwość ich modyfikacji;
3) poziom III — wprowadzenie, modyfikacja oraz usuwanie danych.

2. Obsługę techniczną nadawania i odbierania uprawnień użytkownikom realizuje minister właściwy do spraw zabezpieczenia społecznego.

3. System zapewnia weryfikacje wprowadzanych danych pod względem formatu oraz poprawności merytorycznej.

§ 5. 1. System wyposaża się w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do przetwarzanych danych.

2. Dla każdego użytkownika rejestrowany jest w systemie odrębny identyfikator i hasło.

3. Bezpośredni dostęp do danych w systemie następuje wyłącznie po wprowadzeniu identyfikatora i hasła użytkownika.

4. Identyfikatora użytkownika nie zmienia się, a po wyrejestrowaniu użytkownika z systemu nie przydziela się go innej osobie.

5. Identyfikator użytkownika, który utracił uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu, unieważnić jego hasło użytkownika oraz podjąć inne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

6. Hasło użytkownika zmieniane jest nie rzadziej niż co 30 dni.

7. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

8. Hasła użytkownika nie udostępnia się również po upływie jego ważności.

§ 6. Osobą odpowiedzialną za bezpieczeństwo danych osobowych zgromadzonych w systemie, w tym w szczególności za przeciwdziałanie dostępowi osób nieuprawnionych do systemu oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemach zabezpieczeń jest administrator danych, zwany dalej „administratorem".

§ 7. W celu zabezpieczenia danych osobowych zgromadzonych w systemie administrator:

1) opracowuje instrukcję, określającą sposób zarządzania systemem z uwzględnieniem wymogów bezpieczeństwa informacji, zawierającą w szczególności:
   a) procedury nadawania użytkownikom systemu uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie oraz wskazanie osoby odpowiedzialnej za wykonywanie tych czynności,
   b) metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem,
   c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
   d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
   e) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w lit. d,
   f) sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu,
   g) procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych;
2) identyfikuje i analizuje zagrożenia i ryzyko, na które może być narażone przetwarzanie danych zgromadzonych w systemie;
3) określa potrzeby w zakresie zabezpieczenia systemu;
4) określa sposoby zabezpieczenia danych osobowych adekwatnie do zagrożeń i ryzyka;
5) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych i ich przetwarzania;
6) wykrywa i reaguje na przypadki naruszenia bezpieczeństwa danych zgromadzonych w systemie.

§ 8. 1. Dane osobowe przetwarzane w systemie zabezpiecza się przez wykonanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

2. Kopie zapasowe należy:

1) przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
2) niezwłocznie usuwać po ustaniu ich użyteczności.

§ 9. System zabezpiecza się w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu;

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

§ 10. 1. Pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe, wyposaża się w zabezpieczenia techniczne uniemożliwiające utratę zbiorów danych osobowych oraz zabezpieczenia chroniące przed dostępem do nich osób nieuprawnionych, wykorzystaniem przez osoby nieuprawnione, uszkodzeniem lub zniszczeniem.

2. Przebywanie osób nieuprawnionych w pomieszczeniach, o których mowa w ust. 1, jest dopuszczalne za zgodą administratora lub w obecności osoby uprawnionej do przetwarzania danych osobowych.

§ 11. 1. System chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych oraz logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

2. Logiczne zabezpieczenia, o których mowa w ust. 1, obejmują:

1) kontrolę przepływu informacji pomiędzy systemem a siecią publiczną;

2) kontrolę działań inicjowanych z sieci publicznej i systemu.

3. Dla danych przesyłanych w sieci publicznej stosuje się środki kryptograficznej ochrony.

§ 12. 1. Dla każdej osoby, której dane są przetwarzane w systemie, system zapewnia spójne odnotowanie:

1) daty wprowadzenia pierwszych i kolejnych danych tej osoby;

2) identyfikatora użytkownika wprowadzającego dane;

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

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, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

§ 13. Urządzenia lub elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora.

§ 14. Urządzenia lub elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do usunięcia z systemu, pozbawia się zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza w sposób uniemożliwiający ich odczytanie.

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

Minister Pracy i Polityki Społecznej: *J. Fedak*