1743

ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI[1)]

z dnia 13 grudnia 2007 r.

w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny

Na podstawie art. 21 ust. 1 ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej (Dz. U. Nr 165, poz. 1170) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) techniczne warunki, sposób i tryb dokonywania wpisów danych SIS;

2) obowiązki uprawnionych organów związane z dokonywaniem wpisów danych SIS;

3) sposób i tryb aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny.

§ 2. Ilekroć w rozporządzeniu jest mowa o:

1) Centralnym Węźle Polskiego Komponentu SIS1+ — należy przez to rozumieć podsystem informacyjny stanowiący część infrastruktury technicznej i organizacyjnej krajowego modułu SIS1+, mający na celu zapewnienie przepływu informacji pomiędzy Centralnym Systemem Informacyjnym Schengen (C.SIS) a krajowymi użytkownikami SISone4ALL;

2) certyfikacie — należy przez to rozumieć elektroniczne zaświadczenie będące elementem PKI, wydane zgodnie z obowiązującą Polityką Certyfikacji, zapewniające poufność przesyłanych danych oraz bezpieczeństwo procesu uwierzytelniania użytkownika instytucjonalnego i użytkownika indywidualnego;

3) GUI SISone4ALL — (Graphical User Interface) — należy przez to rozumieć sposób prezentacji graficznej informacji oraz interakcji z użytkownikiem;

4) interfejsie SISone4ALL — należy przez to rozumieć interfejs programu użytkownika;

5) Kodeksie Postępowania Certyfikacyjnego — należy przez to rozumieć dokument uszczegółowiający ogólne zasady postępowania certyfikacyjnego opisane w Polityce Certyfikacji;

6) wartościach katalogowych — należy przez to rozumieć kodowany słownik danych będący zbiorem określonych dopuszczalnych wartości lub terminów wykorzystywanych przez interfejs SISone4ALL;

7) PKI — (Public Key Infrastructure) — należy przez to rozumieć Infrastrukturę Klucza Publicznego będącego kryptosystemem, w którego skład wchodzą urzędy certyfikacyjne, urzędy rejestracyjne, użytkownicy certyfikatów (subskrybenci), oprogramowanie i sprzęt;

8) Polityce Certyfikacji — należy przez to rozumieć dokument określający techniczne i organizacyjne warunki oraz zakres tworzenia i stosowania certyfikatów w standardzie X.509 wykorzystywanych przez użytkowników SIS1+;

9) sieć SDH — należy przez to rozumieć synchroniczną, cyfrową sieć miejską w Warszawie, będącą w dyspozycji ministra właściwego do spraw wewnętrznych, która realizuje funkcje wspólnej platformy teleinformatycznej łączącej narodowy centralny węzeł SISone4ALL z krajowymi użytkownikami instytucjonalnymi oraz międzynarodową siecią SISNet;

10) SIS1+ — należy przez to rozumieć zmodernizowany System Informacyjny Schengen pierwszej generacji;

11) SISone4ALL — należy przez to rozumieć specjalistyczne rozwiązanie informatyczne umożliwiające obsługę SIS1+;

12) SSL — (Secure Socket Layer) — należy przez to rozumieć protokół służący do szyfrowania transmisji danych w sieci;

13) translatorze — należy przez to rozumieć moduł umożliwiający tłumaczenie zapytań i odpowiedzi, przesyłanych pomiędzy użytkownikami instytucjonalnymi a Centralnym Węzłem Polskiego Komponentu SIS1+, z zaadaptowanego formatu Systemu Informacyjnego Schengen drugiej generacji na protokół obowiązujący w SISone4ALL;

14) transliteracji — należy przez to rozumieć sposób zapisywania tekstu pisanego w jednym alfabecie znakami innego alfabetu, zgodnie z ustalonym ich znaczeniem, zapewniający ścisłą odpowiedniość obu tekstów;

15) ustawie — należy przez to rozumieć ustawę z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej;

16) użytkowniku indywidualnym — należy przez to rozumieć osobę fizyczną uprawnioną w ramach organu lub służby do wykorzystywania danych SIS, która w celu dostępu do danych korzysta bezpośrednio z GUI SISone4ALL;

[1)] Minister Spraw Wewnętrznych i Administracji kieruje działem administracji rządowej — sprawy wewnętrzne, na podstawie § 1 ust. 2 pkt 3 rozporządzenia Prezesa Rady Ministrów z dnia 16 listopada 2007 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (Dz. U. Nr 216, poz. 1604).

17) użytkowniku instytucjonalnym — należy przez to rozumieć organ lub służbę, uprawnione do współpracy z Krajowym Systemem Informatycznym za pośrednictwem własnego systemu informatycznego;

18) użytkowniku końcowym — należy przez to rozumieć osobę fizyczną uprawnioną w ramach organu lub służby do wykorzystywania danych SIS, posiadającą dostęp do Krajowego Systemu Informatycznego za pośrednictwem systemu informatycznego użytkownika instytucjonalnego;

19) VPN — (Virtual Private Network) — należy przez to rozumieć wirtualną sieć prywatną jako sieć przekazu danych korzystającą z publicznej infrastruktury telekomunikacyjnej, która poprzez stosowanie protokołów tunelowania i procedur bezpieczeństwa zachowuje poufność danych;

20) X.509 — należy przez to rozumieć standard opisujący sposób użycia asymetrycznych algorytmów kryptograficznych.

§ 3. 1. Użytkownik indywidualny dokonuje w SIS1+ wpisów danych SIS z wykorzystaniem protokołu https oraz GUI SISone4ALL, wykorzystując w tym celu bezpieczne połączenie VPN.

2. Dokonywanie wpisów danych SIS następuje, z zastrzeżeniem ust. 3, za pośrednictwem fizycznie wydzielonej sieci teleinformatycznej, która nie ma styku z siecią ogólnodostępną.

3. W przypadku polskich urzędów konsularnych dokonywanie wpisów danych SIS następuje za pośrednictwem wydzielonych do tego stanowisk, wyposażonych w mechanizmy szyfrujące zapewniające bezpieczeństwo przekazu informacji oraz poufność i integralność przekazywanych danych, zgodnie z przepisami dotyczącymi ochrony danych osobowych oraz bezpieczeństwa teleinformatycznego.

4. W celu zabezpieczenia dostępu użytkownika indywidualnego do SIS1+ wykorzystuje się technologię SSL z wykorzystaniem certyfikatów X.509.

5. Za bezpieczeństwo w sieci teleinformatycznej Centralnego Węzła Polskiego Komponentu SIS1+ odpowiada centralny organ techniczny KSI, natomiast za bezpieczeństwo w sieci SDH odpowiada minister właściwy do spraw wewnętrznych.

6. W celu umożliwienia dokonywania wpisów danych SIS organ lub służba korzystające bezpośrednio z GUI SISone4ALL występują do centralnego organu technicznego KSI o:

1) wydanie certyfikatów dla brzegowego urządzenia sieciowego oraz określenie i przekazanie parametrów konfiguracji brzegowego urządzenia sieciowego dla użytkownika indywidualnego, umożliwiającego bezpieczne nawiązanie połączenia z SIS1+;

2) przekazywanie aktualnie obowiązującej Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego;

3) założenie kont dostępowych i przydzielenie uprawnień w SISone4ALL dla użytkowników indywidualnych.

§ 4. 1. Użytkownik instytucjonalny dokonuje w SIS1+ wpisów danych SIS z wykorzystaniem własnego systemu informatycznego z użyciem protokołu https oraz interfejsu SISone4ALL oraz bezpiecznego połączenia VPN.

2. Dokonywanie wpisów danych SIS następuje za pośrednictwem wydzielonej sieci teleinformatycznej, która nie ma fizycznego styku z siecią ogólnodostępną.

3. W celu zabezpieczenia dostępu użytkownika instytucjonalnego do SIS1+ wykorzystuje się technologię SSL z wykorzystaniem certyfikatów X.509.

4. W celu umożliwienia dokonywania wpisów danych SIS użytkownik instytucjonalny występuje do centralnego organu technicznego KSI o:

1) wydanie certyfikatów dla brzegowego urządzenia sieciowego i serwerów systemu informatycznego użytkownika instytucjonalnego oraz określenie i przekazanie parametrów konfiguracji brzegowego urządzenia sieciowego umożliwiającego bezpieczne nawiązanie połączenia z SIS1+;

2) przekazywanie aktualnie obowiązującej Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego;

3) przekazanie niezbędnej dokumentacji zawierającej specyfikację interfejsu translatora.

§ 5. Do obowiązków organu lub służby korzystających bezpośrednio z GUI SISone4ALL oraz użytkownika instytucjonalnego, w zakresie technicznych warunków dokonywania wpisów danych SIS należy:

1) przestrzeganie zasad obowiązujących w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego;

2) zapewnienie bezpieczeństwa w swojej sieci teleinformatycznej, podłączonej do Centralnego Węzła Polskiego Komponentu SIS1+.

§ 6. 1. Wpisów danych SIS do SIS1+ dokonuje się:

1) za pomocą GUI SISone4ALL — w przypadku użytkownika indywidualnego;

2) za pomocą systemu informatycznego użytkownika instytucjonalnego — w przypadku użytkownika końcowego.

2. W przypadku braku bezpośredniego dostępu do Krajowego Systemu Informatycznego spowodowanego przyczynami niezależnymi od danego użytkownika instytucjonalnego lub użytkownika indywidualnego użytkownik instytucjonalny lub użytkownik indywidualny przesyła odpowiednią wypełnioną kartę wpisu danych SIS do SIS1+ centralnemu organowi technicznemu KSI w sposób zapewniający uwierzytelnienie przekazu informacji oraz poufność i integralność przekazywanych danych, zgodnie z przepisami dotyczącymi ochrony danych osobowych oraz bezpieczeństwa teleinformatycznego.

3. Do obowiązków organu lub służby korzystających bezpośrednio z GUI SISone4ALL oraz użytkownika instytucjonalnego, w zakresie sposobu dokonywania wpisów danych SIS należy:

1) sprawdzenie przed dokonaniem wpisu, czy dana osoba lub przedmiot już figuruje w SIS1+, oraz, w przypadku pozytywnego wyniku sprawdzenia, przeprowadzenie niezbędnych konsultacji mających na celu zapobieżenie powstaniu niezgodności wpisów wielokrotnych:
   a) za pośrednictwem Biura SIRENE — w przypadku wpisów dokonanych przez inne państwa członkowskie Unii Europejskiej,
   b) bezpośrednio z krajowym organem, który dokonał wpisu, a w przypadku braku możliwości przeprowadzenia bezpośrednich konsultacji — za pośrednictwem centralnego organu technicznego KSI;
2) stosowanie zasad transliteracji i wartości katalogowych, określonych i udostępnionych przez centralny organ techniczny KSI;
3) zapewnienie legalności, aktualności i zgodności z celami dokonywanych wpisów;
4) niezwłoczne dokonywanie wpisów.

4. W przypadku gdy użytkownik indywidualny lub użytkownik instytucjonalny jest uprawniony do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych SIS należących do jednej z kategorii danych określonych w art. 3 ust. 1 ustawy, a jednocześnie nie jest uprawniony do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu wglądu do tej samej kategorii danych na podstawie art. 4 ust. 1 ustawy, wówczas sprawdzenia i konsultacje, o których mowa w ust. 3 pkt 1, prowadzi za pośrednictwem centralnego organu technicznego KSI.

§ 7. 1. W przypadku użytkownika indywidualnego wprowadza się następujący tryb dokonywania wpisów danych SIS:

1) dokonanie autoryzacji w GUI SISone4ALL na podstawie przydzielonego konta zabezpieczonego hasłem;
2) dokonanie wpisu, zgodnie z przydzielonymi uprawnieniami;
3) po dokonaniu wpisu — wylogowanie się z GUI SISone4ALL.

2. W przypadku użytkownika końcowego wprowadza się następujący tryb dokonywania wpisów danych SIS:

1) uwierzytelnienie użytkownika końcowego w systemie informatycznym na podstawie przydzielonych uprawnień;
2) dokonanie wpisu przez użytkownika końcowego zgodnie z przydzielonymi uprawnieniami;
3) automatyczne przekazanie informacji do SIS1+ przez system informatyczny;
4) odnotowanie w elektronicznym rejestrze informacji dotyczących:
   a) użytkownika końcowego, ze wskazaniem jego jednostki i komórki organizacyjnej,
   b) daty i godziny dokonania wpisu,
   c) danych SIS,
   d) niepowtarzalnego identyfikatora wpisu nadanego przez Krajowy System Informatyczny,
   e) rodzaju czynności wykonanej za pośrednictwem Krajowego Systemu Informatycznego,
   f) kryteriów wyszukiwania,
   g) listy wyników wyszukiwania, do których uzyskał dostęp użytkownik końcowy.

3. Do obowiązków organu lub służby korzystających bezpośrednio z GUI SISone4ALL oraz użytkownika instytucjonalnego, w zakresie trybu dokonywania wpisów danych SIS należy zapewnienie, aby użytkownicy indywidualni i użytkownicy końcowi:

1) dokonywali wpisów w sposób zapewniający ich legalność i poufność;
2) zachowywali bezpieczeństwo procesu uwierzytelniania.

4. Do obowiązków użytkownika instytucjonalnego, w zakresie trybu dokonywania wpisów danych SIS należy:

1) zapewnienie prowadzenia elektronicznego rejestru, o którym mowa w ust. 2 pkt 4;
2) niezwłoczne udostępnienie — na żądanie Generalnego Inspektora Ochrony Danych Osobowych lub ministra właściwego do spraw wewnętrznych — rejestru, o którym mowa w ust. 2 pkt 4.

§ 8. Aktualizowanie, usuwanie i wyszukiwanie danych SIS poprzez Krajowy System Informatyczny odbywa się z wykorzystaniem:

1) GUI SISone4ALL oraz z zastosowaniem zasad transliteracji przez:
   a) użytkownika indywidualnego,
   b) centralny organ techniczny KSI — w przypadku określonym w art. 22 ust. 2 ustawy;
2) systemu informatycznego użytkownika instytucjonalnego przez użytkownika końcowego.

§ 9. Do aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny stosuje się odpowiednio § 7 ust. 1 i 2.

§ 10. Rozporządzenie wchodzi w życie z dniem ogłoszenia.

Minister Spraw Wewnętrznych i Administracji:
G. Schetyna