



DZIENNIK USTAW

RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 5 kwietnia 2013 r.

Poz. 426

ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH¹⁾

z dnia 3 kwietnia 2013 r.

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

Na podstawie art. 21 ust. 1 ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz. U. Nr 165, poz. 1170, z późn. zm.²⁾) 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, zwany dalej „KSI”.

§ 2. Ilekroć w rozporządzeniu jest mowa o:

- 1) aplikacji WWW SIS – należy przez to rozumieć graficzny interfejs użytkownika KSI, wykorzystywany do aktualizowania, usuwania i wyszukiwania danych SIS;
- 2) Centralnym Węźle Polskiego Komponentu SIS (CWPK SIS) – należy przez to rozumieć podsystem informacyjny stanowiący część infrastruktury technicznej i organizacyjnej KSI, mający na celu zapewnienie przepływu informacji pomiędzy centralnym systemem SIS (CS SIS) a Systemami Centralnymi Użytkowników Instytucjonalnych;
- 3) 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;
- 4) organie lub służbie – należy przez to rozumieć organ lub służbę uprawnione do bezpośredniego dostępu do KSI, na podstawie ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym;
- 5) Kodeksie Postępowania Certyfikacyjnego – należy przez to rozumieć dokument uszczegółwiający 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 SIS;

¹⁾ Minister Spraw Wewnętrznych kieruje działem administracji rządowej – sprawy wewnętrzne, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2011 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych (Dz. U. Nr 248, poz. 1491).

²⁾ Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. Nr 195, poz. 1198 i Nr 216, poz. 1367, z 2010 r. Nr 41, poz. 233, Nr 81, poz. 531 i Nr 239, poz. 1593.

- 7) PKI (Public Key Infrastructure) – należy przez to rozumieć Infrastrukturę Klucza Publicznego będącego kryptosystemem, w którego skład wchodzi 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 SIS;
- 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 SIS z krajowymi użytkownikami instytucjonalnymi oraz międzynarodową siecią SISNet;
- 10) SSL (Secure Socket Layer) – należy przez to rozumieć protokół służący do szyfrowania transmisji danych w sieci;
- 11) translatorze – należy przez to rozumieć moduł umożliwiający tłumaczenie zapytań i odpowiedzi, przesyłanych pomiędzy użytkownikami instytucjonalnymi a CWPK SIS;
- 12) 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;
- 13) ustawie – należy przez to rozumieć ustawę z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym;
- 14) użytkownika indywidualnym – należy przez to rozumieć osobę fizyczną upoważnioną w ramach organu lub służby do wykorzystywania danych poprzez KSI, która w celu dostępu do danych SIS korzysta bezpośrednio z aplikacji WWW SIS;
- 15) użytkownika instytucjonalnym – należy przez to rozumieć organ lub służbę uprawnione do współpracy z KSI za pośrednictwem własnego systemu teleinformatycznego;
- 16) użytkownika końcowym – należy przez to rozumieć osobę fizyczną upoważnioną do wykorzystywania danych poprzez KSI, za pośrednictwem systemu teleinformatycznego użytkownika instytucjonalnego;
- 17) VPN (Virtual Private Network) – należy przez to rozumieć wirtualną sieć prywatną jako sieć przekazu danych korzystającą z publicznej infrastruktury telekomunikacyjnej, która dzięki stosowaniu protokołów tunelowania i procedur bezpieczeństwa zachowuje poufność danych;
- 18) wydzielonej sieci teleinformatycznej – należy przez to rozumieć niepubliczną sieć telekomunikacyjną, która dzięki zastosowaniu rozwiązań sprzętowych lub programowych zapewnia możliwość logicznej separacji od powszechnie dostępnej infrastruktury telekomunikacyjnej;
- 19) X.509 – należy przez to rozumieć standard opisujący sposób użycia asymetrycznych algorytmów kryptograficznych.

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

2. Dokonywanie wpisów danych SIS następuje za pośrednictwem wydzielonej sieci teleinformatycznej.

3. W celu zabezpieczenia dostępu użytkownika indywidualnego do SIS wykorzystuje się technologię SSL z wykorzystaniem certyfikatów X.509.

4. Za bezpieczeństwo w sieci teleinformatycznej CWPK SIS odpowiada centralny organ techniczny KSI, natomiast za bezpieczeństwo w sieci SDH odpowiada minister właściwy do spraw wewnętrznych.

5. W celu umożliwienia dokonywania wpisów danych SIS organ lub służba 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 SIS;
- 2) przekazywanie aktualnie obowiązującej Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego;
- 3) założenie kont dostępowych i przydzielenie uprawnień w SIS użytkownikom indywidualnym;
- 4) wydanie certyfikatów cyfrowych na potrzeby uwierzytelniania się użytkowników indywidualnych w KSI.

§ 4. 1. Użytkownik końcowy dokonuje w SIS wpisów danych SIS z użyciem protokołu https oraz bezpiecznego połączenia VPN.

2. Dokonywanie wpisów danych SIS następuje za pośrednictwem wydzielonej sieci teleinformatycznej.

3. W celu zabezpieczenia dostępu użytkownika instytucjonalnego do SIS 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 SIS;
- 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 aplikacji WWW SIS 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 CWPK SIS.

§ 6. 1. Wpisów danych do SIS dokonuje się odpowiednio:

- 1) za pomocą aplikacji WWW SIS – w przypadku użytkownika indywidualnego;
- 2) za pomocą systemu informatycznego użytkownika instytucjonalnego – w przypadku użytkownika końcowego.

2. W przypadku braku bezpośredniego dostępu do KSI spowodowanego przyczynami niezależnymi od danego organu lub służby organ lub służba kierują wnioskiem o dokonanie wpisu danych SIS na wypełnionej karcie wpisu do centralnego organu technicznego 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 aplikacji WWW SIS oraz użytkownika instytucjonalnego w zakresie sposobu dokonywania wpisów danych SIS należy:

- 1) sprawdzenie przed dokonaniem wpisu, czy dana osoba lub przedmiot już figuruje w SIS, oraz, w przypadku pozytywnego wyniku sprawdzenia, przeprowadzenie niezbędnych konsultacji zgodnie z zasadami określonymi w podręczniku SIRENE, mających na celu zapobieżenie powstaniu niezgodności wpisów wielokrotnych:
 - a) za pośrednictwem Biura SIRENE – w przypadku wpisów dokonanych przez inne państwa członkowskie,
 - 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 aktualizowania i usuwania wpisów.

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

- 1) dokonanie uwierzytelnienia na podstawie otrzymanego certyfikatu cyfrowego przechowywanego na karcie mikroprocesorowej zabezpieczonej PIN-em;
- 2) dokonanie wpisu, zgodnie z przydzielonymi uprawnieniami;
- 3) po dokonaniu wpisu – wylogowanie się z aplikacji WWW SIS.

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 SIS przez system informatyczny;
- 4) automatyczne 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 KSI,
 - e) rodzaju czynności wykonanej za pośrednictwem KSI,
 - f) kryteriów wyszukiwania,
 - g) listy wyników wyszukiwania, do których uzyskał dostęp użytkownik końcowy.

3. Do obowiązków organu lub służby korzystających bezpośrednio z aplikacji WWW SIS 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 KSI odbywa się z wykorzystaniem:

- 1) aplikacji WWW SIS 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 KSI stosuje się odpowiednio § 7 ust. 1 i 2.

§ 10. Traci moc rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 grudnia 2007 r. w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny (Dz. U. Nr 236, poz. 1743).

§ 11. Rozporządzenie wchodzi w życie z dniem określonym w decyzji Rady, zgodnie z art. 55 ust. 2 rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz. Urz. UE L 381 z 28.12.2006, str. 4).³⁾

Minister Spraw Wewnętrznych: *B. Sienkiewicz*

³⁾ Zgodnie z decyzją Rady z dnia 7 marca 2013 r. ustalającą datę rozpoczęcia stosowania rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady w sprawie utworzenia, funkcjonowania i użytkowania systemu informacyjnego Schengen drugiej generacji (SIS II) (Dz. Urz. UE 2013, poz. 158) niniejsze rozporządzenie wchodzi w życie z dniem 9 kwietnia 2013 r.