Projekt z dnia

15 stycznia 2013 r.

ROZPORZĄDZENIE

MINISTRA SPRAW WEWNĘTRZNYCH[1)]

z dnia ..... 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 (KSI).

§ 2. Ilekroć w rozporządzeniu jest mowa o:

1) Centralnym Węźle Polskiego Komponentu SIS (CW PK SIS II) – należy przez to rozumieć podsystem informacyjny stanowiący część infrastruktury technicznej i organizacyjnej Krajowego Systemu Informatycznego (KSI), mający na celu zapewnienie przepływu informacji pomiędzy centralnym systemem SIS (CS SIS II) a Systemami Centralnymi Użytkowników Instytucjonalnych;
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;

[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.

3) organie lub służbie – należy przez to rozumieć organ lub służbę uprawnioną do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI), na podstawie ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym;
4) Kodeksie Postępowania Certyfikacyjnego – należy przez to rozumieć dokument uszczegółowiający ogólne zasady postępowania certyfikacyjnego opisane w Polityce Certyfikacji;
5) wartościach katalogowych – należy przez to rozumieć kodowany słownik danych będący zbiorem określonych dopuszczalnych wartości lub terminów wykorzystywanych przez interfejs SIS;
6) 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;
7) 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;
8) sieć wydzielona – 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;
9) SSL - (Secure Socket Layer) – należy przez to rozumieć protokół służący do szyfrowania transmisji danych w sieci;
10) translatorze - należy przez to rozumieć moduł umożliwiający tłumaczenie zapytań i odpowiedzi, przesyłanych pomiędzy użytkownikami instytucjonalnymi a Centralnym Węzłem Polskiego Komponentu SIS,
11) 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;
12) ustawie – należy przez to rozumieć ustawę z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym;

13) użytkowniku indywidualnym – należy przez to rozumieć osobę fizyczną upoważnioną w ramach organu lub służby do wykorzystywania danych poprzez Krajowy System Informatyczny (KSI), która w celu dostępu do danych SIS korzysta bezpośrednio z aplikacji WWW SIS;

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

15) użytkowniku końcowym – należy przez to rozumieć osobę fizyczną upoważnioną do wykorzystywania danych, poprzez Krajowy System Informatyczny (KSI) za pośrednictwem systemu teleinformatycznego użytkownika instytucjonalnego;

16) 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;

17) X.509 – należy przez to rozumieć standard opisujący sposób użycia asymetrycznych algorytmów kryptograficznych;

18) aplikacja WWW SIS – należy przez to rozumieć graficzny interfejs użytkownika Krajowego Systemu Informatycznego (KSI), wykorzystywany do aktualizowania, usuwania i wyszukiwania danych SIS.

§ 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, z zastrzeżeniem ust. 3, za pośrednictwem fizycznie wydzielonej sieci teleinformatycznej.

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 SIS wykorzystuje się technologię SSL z wykorzystaniem certyfikatów X.509.

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

6. 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 dla użytkowników indywidualnych.

§ 4. 1. Użytkownik instytucjonalny dokonuje w SIS wpisów danych SIS z wykorzystaniem własnego systemu informatycznego 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 Centralnego Węzła Polskiego Komponentu 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 Krajowego Systemu Informatycznego (KSI) spowodowanego przyczynami niezależnymi od danego organu lub służby, organ lub służba kierują wniosek 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 autoryzacji w aplikacji WWW SIS na podstawie przydzielonego konta zabezpieczonego hasłem;

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) 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 (KSI),

e) rodzaju czynności wykonanej za pośrednictwem Krajowego Systemu Informatycznego (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 Krajowy System Informatyczny (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 Krajowy System Informatyczny (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 PE 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).

UZASADNIENIE

W związku z trwającymi pracami nad wdrożeniem Systemu Informacyjnego Schengen drugiej generacji (SIS II), istnieje konieczność zmiany rozporządzenia 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).

Na podstawie 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) oraz decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) każdy kraj uczestniczący w realizacji zadań wynikających z Konwencji Wykonawczej do Układu Schengen zobowiązany jest do przygotowania rozwiązań w zakresie zmian warstwy technicznej i informacyjnej Krajowych Komponentów Systemu Informacyjnego Schengen.

Na podstawie przywołanych wyżej aktów prawa europejskiego zmiany muszą być wprowadzone w prawie krajowym, gdyż stanowią one podstawę modernizacji Polskiego Komponentu Systemu Informacyjnego Schengen w tym w szczególności zmian związanych z funkcjonowaniem Krajowego Systemu Informatycznego.

Wymagane jest wprowadzenie uzupełnienia przyjętych definicji oraz nazewnictwa, celem dostosowania do nowych rozwiązań technicznych oraz zakresu informacyjnego zgodnie z przywołanymi wyżej regulacjami unijnymi.

Zmianie ulegną nazwy opisujące elementy systemu informacyjnego w warstwie technicznej i informacyjnej. Ich wyjaśnienie zostało zawarte w § 2 projektu zawierającym definicje zastosowanych w rozporządzeniu wyrażeń.

W § 3 określono techniczne warunki dokonywania wpisów danych SIS przez użytkownika indywidualnego, natomiast w § 4 przez użytkownika instytucjonalnego. Obowiązki organu lub służby korzystających bezpośrednio z aplikacji WWW SIS oraz obowiązki użytkownika instytucjonalnego, w zakresie technicznych warunków dokonywania wpisów danych SIS określa § 5 rozporządzenia.

W § 7 ust. 1 określono tryb dokonywania wpisów danych SIS przez użytkownika indywidualnego, począwszy od autoryzacji hasłem a zakończywszy na wylogowaniu. Natomiast ust. 2 tego przepisu określa tryb dokonywania wpisów przez użytkownika końcowego.

Techniczne warunki niezbędne do aktualizowania, usuwania i wyszukiwania danych SIS określa § 8.

W związku z tym, iż zmiany będą obejmowały znaczną część rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 13 grudnia 2007 r. zasadnym jest wydanie nowego rozporządzenia.

Z uwagi na fakt, iż System Informacyjny Schengen drugiej generacji nie został jeszcze wdrożony i nie została określona data jego uruchomienia, istnieje konieczność wprowadzenia terminu określającego wejście w życie rozporządzenia z dniem wskazanym 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).

Rozporządzenie nie zawiera przepisów technicznych, a zatem nie podlega notyfikacji, zgodnie z trybem przewidzianym w przepisach rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039, z późn. zm.).

WSTĘPNA OPINIA
O ZGODNOŚCI PROJEKTU Z PRAWEM UNII EUROPEJSKIEJ

Na podstawie § 10 ust. 7 uchwały nr 49 Rady Ministrów z dnia 19 marca 2002 r. – Regulamin pracy Rady Ministrów (M. P. Nr 13, poz. 221, z późn. zm.) przedstawia się następującą opinię:

Analiza przepisów zawartych w projekcie *rozporządzenia Ministra Spraw Wewnętrznych w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informacyjny* wykazuje, że jest on zgodny z prawem Unii Europejskiej.

OCENA SKUTKÓW REGULACJI

1. **Podmioty, na które oddziałuje projektowana regulacja.**

Przepisy projektowanego rozporządzenia będą oddziaływać na organy uprawnione do bezpośredniego i pośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu dokonywania wpisów oraz wglądu do danych SIS, które zostały wskazane w ustawie 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. **Konsultacje społeczne.**

Treść projektowanego rozporządzenia zostanie zamieszcza zgodnie art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414 oraz z 2009 r. Nr 42, poz. 337) – w wersji elektronicznej w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Spraw Wewnętrznych.

Projekt zostanie także zamieszczony na stronie podmiotowej Rządowego Centrum Legislacji w zakładce Rządowy Proces Legislacyjny.

3. **Wpływ regulacji na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego.**

Dostosowanie systemu będzie realizowane przez Biuro Łączności i Informatyki Komendy Głównej Policji, a nie przez firmę zewnętrzną, w związku z tym koszty, jakie będą ponoszone w ramach nowelizacji przedmiotowego rozporządzenia zostaną ograniczone do kosztów wynagrodzeń pracowników Biura Łączności i Informatyki Komendy Głównej Policji.

Dodatkowe środki finansowe, związane m.in. z zakupem sprzętu teleinformatycznego, zabezpieczone zostaną w ramach obecnie prowadzonego projektu pod nazwą „Modernizacja KSI" finansowanego z Funduszu Granic Zewnętrznych. Wartość wkładu własnego wynosi 7 053 750 zł. Powyższa kwota została ujęta w rozdziale 75495 § 6060 projektu planu rzeczowego Biura Łączności i Informatyki Komendy Głównej Policji na 2013 rok.

4. **Wpływ na rynek pracy.**

Wdrożenie projektowanego aktu prawnego nie będzie miało wpływu na rynek pracy.

5. **Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw.**

Projektowane rozporządzenie nie będzie miało bezpośredniego wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw.

6. **Wpływ regulacji na sytuację i rozwój regionalny.**

Wejście w życie rozporządzenia nie będzie miało wpływu na sytuację i rozwój regionalny.

Za zgodność
pod względem prawnym
i redakcyjnym

DYREKTOR
Departamentu Prawnego
Ministerstwa Spraw Wewnętrznych
Andrzej RUBLICKI