DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 20 listopada 2018 r.

Poz. 2162

OBWIESZCZENIE
MARSZAŁKA SEJMU RZECZYPOSPOLITEJ POLSKIEJ

z dnia 25 października 2018 r.

w sprawie ogłoszenia jednolitego tekstu ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym

1. Na podstawie art. 16 ust. 1 zdanie pierwsze ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2017 r. poz. 1523) ogłasza się w załączniku do niniejszego obwieszczenia jednolity tekst ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz. U. z 2018 r. poz. 134), z uwzględnieniem zmian wprowadzonych ustawą z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz. 138) oraz zmian wynikających z przepisów ogłoszonych przed dniem 24 października 2018 r.

2. Podany w załączniku do niniejszego obwieszczenia tekst jednolity ustawy nie obejmuje art. 357, art. 376 i art. 392 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz. 138), które stanowią:

„Art. 357. 1. Decyzje, postanowienia, poświadczenia bezpieczeństwa i odmowy wydania poświadczenia bezpieczeństwa wydane przez pełnomocnika ochrony informacji niejawnych BOR zachowują ważność, chyba że na podstawie odrębnych przepisów zostaną zmienione lub utracą ważność.

2. Akredytacje systemów teleinformatycznych udzielone dla systemów teleinformatycznych użytkowanych przez BOR przed dniem wejścia w życie niniejszej ustawy zachowują ważność do czasu dokonania w systemie teleinformatycznym zmian, które mogą mieć istotny wpływ na bezpieczeństwo teleinformatyczne, lub upływu terminu ich ważności.”

„Art. 376. Dotychczasowe upoważnienia Szefa BOR wydane odpowiednio funkcjonariuszom albo pracownikom w celu wykonywania przez nich obowiązków służbowych oraz zadań, stają się upoważnieniami Komendanta SOP, na okres nie dłuższy niż do dnia następującego po upływie 3 miesięcy od dnia wejścia w życie niniejszej ustawy.”

„Art. 392. Ustawa wchodzi w życie z dniem 1 lutego 2018 r., z wyjątkiem art. 346, który wchodzi w życie z dniem ogłoszenia.”.

Marszałek Sejmu: *M. Kuchciński*

Załącznik do obwieszczenia Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 25 października 2018 r. (poz. 2162)

USTAWA

z dnia 24 sierpnia 2007 r.

o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym

Rozdział 1

Przepisy ogólne

Art. 1. Ustawa określa zasady i sposób realizacji udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, w tym obowiązki i uprawnienia organów dotyczące dokonywania wpisów oraz wglądu do danych zawartych w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym poprzez Krajowy System Informatyczny (KSI).

Art. 2. Ilekroć w ustawie jest mowa o:

1) bezpośrednim dostępie – rozumie się przez to dokonywanie wpisów oraz wgląd do danych wykorzystywanych poprzez Krajowy System Informatyczny (KSI), realizowany w sposób bezpośredni przez organ wskazany w ustawie;

2) Centralnym Wizowym Systemie Informacyjnym – rozumie się przez to system centralny, o którym mowa w art. 1 ust. 2 decyzji Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS) (Dz. Urz. UE L 213 z 15.06.2004, str. 5–7);

3) centralnym organie technicznym KSI – rozumie się przez to Komendanta Głównego Policji;

4) danych – rozumie się przez to dane SIS lub dane VIS;

5) danych SIS – rozumie się przez to dane określone w art. 20 ust. 1 i 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) oraz dane określone w art. 20 ust. 1–3 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz. Urz. UE L 205 z 07.08.2007, str. 63);

6) danych VIS – rozumie się przez to dane określone w art. 5 ust. 1 rozporządzenia (WE) nr 767/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS) (Dz. Urz. UE L 218 z 13.08.2008, str. 60–81);

7) informacjach uzupełniających – rozumie się przez to wszelkie informacje, wymieniane za pośrednictwem biur SIRENE między krajowymi a zagranicznymi organami uprawnionymi do wykorzystywania danych SIS, niezbędne przy dokonywaniu wpisów do Systemu Informacyjnego Schengen lub w celu umożliwienia podjęcia odpowiednich działań, w przypadkach gdy w wyniku przeglądania danych SIS odnaleziono osoby lub przedmioty, których dotyczą wpisy;

8) interfejsie krajowym – rozumie się przez to interfejs krajowy, o którym mowa w art. 1 ust. 2 decyzji Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego;

9) (uchylony)

10) kopii krajowej – rozumie się przez to pełną kopię bazy danych SIS, o której mowa w art. 4 ust. 1 lit. b 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 w art. 4 ust. 1 lit. b decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II);

11) Krajowym Systemie Informatycznym (KSI) – rozumie się przez to zespół współpracujących ze sobą urządzeń, procedur przetwarzania informacji i narzędzi programowych (oprogramowania) zastosowanych w celu przetwarzania danych oraz infrastrukturę telekomunikacyjną, umożliwiające organom administracji publicznej i organom wymiaru sprawiedliwości wykorzystywanie danych gromadzonych w Systemie Informacyjnym Schengen oraz w Wizowym Systemie Informacyjnym;

12) (uchylony)

13) Państwie Członkowskim – rozumie się przez to państwo członkowskie Unii Europejskiej, państwo członkowskie Europejskiego Porozumienia o Wolnym Handlu (EFTA) – strony umowy o Europejskim Obszarze Gospodarczym nienależące do Unii Europejskiej lub państwo niebędące stroną umowy o Europejskim Obszarze Gospodarczym, którego obywatele mogą korzystać ze swobody przepływu osób na podstawie umów zawartych przez to państwo ze Wspólnotą Europejską i jej państwami członkowskimi, z wyjątkiem państwa, wobec którego Rada podjęła decyzję o niestosowaniu przepisów dorobku Schengen;

14) pośrednim dostępie – rozumie się przez to dokonywanie wpisów oraz wgląd do danych wykorzystywanych poprzez Krajowy System Informatyczny (KSI), realizowany w sytuacjach wskazanych w ustawie za pośrednictwem centralnego organu technicznego KSI albo organu wskazanego w art. 7 ust. 2;

14a) systemie centralnym SIS II – rozumie się przez to system centralny składający się z funkcji wsparcia technicznego zawierającej bazę danych oraz z jednolitego interfejsu krajowego, o którym mowa w art. 4 ust. 1 lit. a 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 w art. 4 ust. 1 lit. a decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II);

15) Systemie Informacyjnym Schengen – rozumie się przez to system informacyjny, o którym mowa w art. 1 i 4 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 w art. 1 i 4 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II);

15a) systemie krajowym N.SIS II – rozumie się przez to polski system krajowy zawierający kopię krajową, który łączy się z systemem centralnym SIS II, o którym mowa w art. 4 ust. 1 lit. b 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 w art. 4 ust. 1 lit. b decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II);

16) Wizowym Systemie Informacyjnym – rozumie się przez to system, o którym mowa w art. 1 decyzji Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS);

17) wpisie – rozumie się przez to czynności faktyczne polegające na wprowadzeniu do Systemu Informacyjnego Schengen lub Wizowego Systemu Informacyjnego, zmianie lub usunięciu z Systemu Informacyjnego Schengen lub Wizowego Systemu Informacyjnego danych umożliwiających właściwym organom identyfikację osoby lub przedmiotu oraz podjęcie wnioskowanego działania w związku ze zidentyfikowaniem osoby lub przedmiotu;

18) wykorzystywaniu danych – rozumie się przez to przetwarzanie danych będących danymi osobowymi w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723)[1)], jak również jakiekolwiek operacje wykonywane na danych niebędących danymi osobowymi, takie jak zbieranie, wpisywanie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

Rozdział 2

Organy i służby uprawnione do wykorzystywania danych

Art. 3. 1. Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu dokonywania wpisów danych SIS dotyczących:

1) osób poszukiwanych do tymczasowego aresztowania w celu wydania ich przez państwo obce na podstawie wniosku o wydanie przysługuje sądowi lub prokuraturze;

2) osób poszukiwanych do tymczasowego aresztowania w celu przekazania osoby ściganej na podstawie europejskiego nakazu aresztowania przysługuje sądowi lub prokuraturze;

[1)] Ustawa utraciła moc z dniem 25 maja 2018 r. z wyjątkiem art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziałów 4, 5 i 7, które zachowują moc w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie, w terminie do dnia wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89), na podstawie art. 175 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000), która weszła w życie z dniem 25 maja 2018 r.

3) świadków wezwanych do stawienia się przed sądem lub prokuratorem w związku z postępowaniem karnym lub postępowaniem karnym skarbowym lub podejrzanych wezwanych do stawienia się przed prokuratorem w związku z postępowaniem karnym lub postępowaniem karnym skarbowym, którzy są poszukiwani, lub oskarżonych wezwanych do stawienia się przed sądem w związku z postępowaniem karnym lub postępowaniem karnym skarbowym w celu poniesienia odpowiedzialności za czyny, za które są poszukiwani, lub skazanych, wobec których powinien zostać wykonany wyrok w sprawie karnej lub w sprawie o przestępstwo skarbowe, lub skazanych wezwanych do stawienia się w celu odbycia kary pozbawienia wolności – dla ustalenia miejsca ich pobytu przysługuje sądowi lub prokuraturze;

4) cudzoziemca, o którym mowa w art. 443 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach (Dz. U. z 2017 r. poz. 2206 i 2282 oraz z 2018 r. poz. 107, 138, 771 i 1669), przysługuje Szefowi Urzędu do Spraw Cudzoziemców;

5) osób zaginionych albo osób zaginionych, które dla ich ochrony lub w celu zapobiegania stwarzanym przez nie zagrożeniom powinny zostać oddane do właściwej placówki opiekuńczej lub leczniczej, przysługuje Policji;

6) osób lub pojazdów silnikowych o pojemności silnika przekraczającej 50 cm^3, statków wodnych, statków powietrznych i kontenerów, wprowadzonych w celu:

   a) przeprowadzania niejawnego nadzorowania, którego celem jest ściganie przestępstw oraz zapobieganie zagrożeniom bezpieczeństwa publicznego, przysługuje Policji, Służbie Celno-Skarbowej, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej lub Centralnemu Biuru Antykorupcyjnemu,

   b) przeprowadzania kontroli, której celem jest ściganie przestępstw oraz zapobieganie zagrożeniom bezpieczeństwa publicznego, przysługuje Policji, Służbie Celno-Skarbowej, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej lub Centralnemu Biuru Antykorupcyjnemu,

   c) przeprowadzania niejawnego nadzorowania, którego celem jest zapobieganie poważnym zagrożeniom wewnętrznego i zewnętrznego bezpieczeństwa państwa, przysługuje Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego lub Służbie Wywiadu Wojskowego,

   d) przeprowadzania kontroli, której celem jest zapobieganie poważnym zagrożeniom wewnętrznego i zewnętrznego bezpieczeństwa państwa, przysługuje Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego lub Służbie Wywiadu Wojskowego;

7) przedmiotów podlegających zatrzymaniu albo zatrzymaniu w celu wykorzystania jako dowód w postępowaniu karnym lub postępowaniu karnym skarbowym przysługuje ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw zagranicznych, Policji, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, wojewodom, Szefowi Urzędu do Spraw Cudzoziemców, dyrektorowi urzędu morskiego, sądowi lub prokuraturze.

2. W przypadku braku bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI), spowodowanego przyczynami niezależnymi od danego organu, organy wymienione w ust. 1 mogą dokonywać wpisów danych SIS za pośrednictwem centralnego organu technicznego KSI.

3. Organy wymienione w ust. 1, dokonując wpisów danych SIS, są obowiązane do zapewnienia ich zgodności z prawem, dokładności i aktualności.

Art. 3a. (uchylony)

Art. 4. 1. Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu wglądu do danych SIS dotyczących:

1) osób poszukiwanych do tymczasowego aresztowania w celu wydania ich na wniosek Państwa Członkowskiego lub państwa obcego przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;

2) osób poszukiwanych do tymczasowego aresztowania w celu przekazania osoby ściganej na podstawie europejskiego nakazu aresztowania przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;

3) świadków wezwanych do stawienia się przed sądem lub prokuratorem w związku z postępowaniem karnym lub postępowaniem karnym skarbowym lub podejrzanych wezwanych do stawienia się przed prokuratorem w związku z postępowaniem karnym lub postępowaniem karnym skarbowym, którzy są poszukiwani, lub oskarżonych wezwanych do stawienia się przed sądem w związku z postępowaniem karnym lub postępowaniem karnym skarbowym w celu poniesienia odpowiedzialności za czyny, za które są poszukiwani, lub skazanych, wobec których powinien

zostać wykonany wyrok w sprawie karnej lub w sprawie o przestępstwo skarbowe, lub skazanych wezwanych do stawienia się w celu odbycia kary pozbawienia wolności – dla ustalenia miejsca ich pobytu przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;

4) cudzoziemców, których dane zostały wpisane do Systemu Informacyjnego Schengen dla celów odmowy wjazdu, przysługuje ministrowi właściwemu do spraw zagranicznych, Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Służbie Celno-Skarbowej, Szefowi Urzędu do Spraw Cudzoziemców, wojewodzie, konsulowi, sądowi lub prokuraturze;

5) osób zaginionych albo osób zaginionych, które dla ich ochrony lub w celu zapobiegania stwarzanym przez nie zagrożeniom powinny być oddane do właściwej placówki opiekuńczej lub leczniczej, przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;

6) osób lub pojazdów silnikowych o pojemności silnika przekraczającej 50 cm^3, statków wodnych, statków powietrznych i kontenerów, wprowadzonych w celu przeprowadzania niejawnego nadzorowania lub kontroli przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Żandarmerii Wojskowej, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;

7) przedmiotów podlegających zatrzymaniu albo zatrzymaniu w celu wykorzystania jako dowód w postępowaniu karnym lub postępowaniu karnym skarbowym, należących do jednej z poniższych kategorii:

   a) pojazdy silnikowe o pojemności silnika przekraczającej 50 cm^3, statki wodne i statki powietrzne,

   b) przyczepy i naczepy o masie własnej przekraczającej 750 kg, przyczepy turystyczne, urządzenia przemysłowe, silniki przyczepne i kontenery,

   c) broń palna,

   d) blankiety dokumentów urzędowych, które zostały skradzione, przywłaszczone lub utracone,

   e) wydane dokumenty tożsamości, takie jak: paszporty, dowody tożsamości, prawa jazdy, dokumenty pobytowe i dokumenty podróży, które zostały skradzione, przywłaszczone, utracone lub unieważnione,

   f) dowody rejestracyjne i tablice rejestracyjne pojazdów, które zostały skradzione, przywłaszczone, utracone lub unieważnione,

   g) banknoty (o spisanych numerach),

   h) papiery wartościowe i środki płatnicze, takie jak: czeki, karty kredytowe, obligacje, akcje i dokumenty potwierdzające udział, które zostały skradzione, przywłaszczone, utracone lub unieważnione

   – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;

8) przedmiotów podlegających zatrzymaniu albo zatrzymaniu w celu wykorzystania jako dowód w postępowaniu karnym lub postępowaniu karnym skarbowym, należących do jednej z kategorii, o których mowa w pkt 7 lit. d oraz e, przysługuje ministrowi właściwemu do spraw wewnętrznych, Szefowi Urzędu do Spraw Cudzoziemców, wojewodzie, konsulowi lub dyrektorowi urzędu morskiego;

9)[2)] przedmiotów podlegających zatrzymaniu albo zatrzymaniu w celu wykorzystania jako dowód w postępowaniu karnym lub postępowaniu karnym skarbowym, należących do jednej z kategorii, o których mowa w pkt 7 lit. a, b oraz f, przysługuje ministrowi właściwemu do spraw wewnętrznych, Służbie Ochrony Państwa, Agencji Wywiadu, Służbie Wywiadu Wojskowego, Służbie Kontrwywiadu Wojskowego, organom jednostek wojskowych Sił Zbrojnych Rzeczypospolitej Polskiej lub wojewodzie mazowieckiemu.

2. Uprawnienie do pośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu wglądu do danych SIS dotyczących przedmiotów, o których mowa w ust. 1 pkt 7 lit. a, b oraz f, przysługuje organom samorządowym właściwym w sprawach rejestracji pojazdów.

[2)] Ze zmianą wprowadzoną przez art. 315 pkt 1 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz. 138), która weszła w życie z dniem 1 lutego 2018 r.

3. Uprawnienie do wglądu do danych SIS przysługuje organom określonym w ust. 1 pkt 9 i ust. 2 wyłącznie w związku z wykonywaniem obowiązku rejestracji pojazdów określonego w art. 73 i 74 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2018 r. poz. 1990) w celu sprawdzenia, czy zgłoszone do rejestracji pojazdy nie zostały skradzione, przywłaszczone lub utracone w inny sposób.

4. Organy, o których mowa w ust. 1 i 2, w przypadku odnalezienia na skutek wglądu do danych SIS osoby lub przedmiotu, których dotyczy wpis, są obowiązane do podjęcia wnioskowanych we wpisie działań, o ile realizowane przez dany organ zadania umożliwiają im takie działania, albo do bezzwłocznego przekazania osoby lub przedmiotu Policji.

5. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, tryb przekazywania Policji osób lub przedmiotów odnalezionych na skutek wglądu do danych SIS, a także związane z tym obowiązki Policji, uwzględniając sprawną i skuteczną realizację wnioskowanych we wpisie działań wobec odnalezionych osób lub przedmiotów.

Art. 4a. (uchylony)

Art. 5. 1. Bezpośredni dostęp do Wizowego Systemu Informacyjnego jest realizowany poprzez Krajowy System Informatyczny (KSI) w celu dokonywania wpisów danych VIS przez Straż Graniczną, konsula, wojewodę, ministra właściwego do spraw zagranicznych lub Szefa Urzędu do Spraw Cudzoziemców.

2. Organy określone w ust. 1 są obowiązane do:

1) wymiany krajowych danych VIS przez dokonywanie wpisów do Centralnego Wizowego Systemu Informacyjnego poprzez Krajowy System Informatyczny (KSI);

2) zapewnienia, aby dokonywane przez dany organ wpisy danych VIS były zgodne z prawem, a ponadto, aby te dane VIS były dokładne i aktualne;

3) zapewnienia usuwania danych VIS po upływie okresu, na który dane te zostały przez dany organ wprowadzone;

4) niezwłocznego informowania centralnego organu technicznego KSI o ujawnionych nieprawidłowościach w związku z wykorzystaniem danych VIS poprzez Krajowy System Informatyczny (KSI);

5) rozpatrzenia wniosków Państw Członkowskich o dokonanie zmiany lub usunięcia danych VIS wprowadzonych przez dany organ oraz powiadomienia Państw Członkowskich o konieczności dokonania zmiany lub usunięcia danych VIS wprowadzonych przez te Państwa Członkowskie.

3. Konsul lub wojewoda niezwłocznie powiadamiają Państwo Członkowskie lub Państwa Członkowskie o nabyciu obywatelstwa polskiego przez osobę ubiegającą się o wizę w tym Państwie Członkowskim lub Państwach Członkowskich.

Art. 6. Bezpośredni dostęp do Wizowego Systemu Informacyjnego realizowany poprzez Krajowy System Informatyczny (KSI) umożliwiający wgląd do danych VIS w celu:

1) rozpatrzenia złożonych wniosków wizowych oraz podjęcia decyzji dotyczących tych wniosków, jak również decyzji o unieważnieniu, przedłużeniu, cofnięciu wizy, przysługuje Straży Granicznej, konsulowi, wojewodzie, ministrowi właściwemu do spraw zagranicznych lub Szefowi Urzędu do Spraw Cudzoziemców;

2) przeprowadzania konsultacji między centralnymi organami wizowymi w sprawie wniosków wizowych zgodnie z art. 22 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiającego Wspólnotowy Kodeks Wizowy (kodeks wizowy) (Dz. Urz. UE L 243 z 15.09.2009, str. 1) przysługuje Szefowi Urzędu do Spraw Cudzoziemców;

3) sporządzania sprawozdań i statystyk, przysługuje Straży Granicznej, konsulowi, wojewodzie, ministrowi właściwemu do spraw zagranicznych lub Szefowi Urzędu do Spraw Cudzoziemców;

4) sprawdzania na przejściach granicznych tożsamości posiadacza wizy, autentyczności wizy lub spełniania warunków wjazdu na terytorium Państw Członkowskich zgodnie z art. 5 rozporządzenia (WE) nr 562/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. ustanawiającego wspólnotowy kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz. Urz. UE L 105 z 13.04.2006, str. 1) przysługuje Straży Granicznej i Służbie Celno-Skarbowej;

5) sprawdzania na terytorium Rzeczypospolitej Polskiej tożsamości posiadacza wizy, autentyczności wizy lub spełniania warunków wjazdu lub pobytu na terytorium Państw Członkowskich przysługuje komendantowi wojewódzkiemu Policji, komendantowi powiatowemu (miejskiemu) Policji, komendantowi oddziału Straży Granicznej lub komendantowi placówki Straży Granicznej, Służbie Celno-Skarbowej, wojewodzie lub Szefowi Urzędu do Spraw Cudzoziemców;

6) zidentyfikowania osoby, która nie spełnia lub przestała spełniać warunki wjazdu lub pobytu na terytorium Państw Członkowskich, przysługuje Straży Granicznej, Policji, Służbie Celno-Skarbowej, wojewodzie lub Szefowi Urzędu do Spraw Cudzoziemców;

7) określania Państwa Członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej zgodnie z art. 12 i art. 34 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca (wersja przekształcona) (Dz. Urz. UE L 180 z 29.06.2013) przysługuje Szefowi Urzędu do Spraw Cudzoziemców;

8) rozpatrzenia wniosku o udzielenie ochrony międzynarodowej przysługuje Szefowi Urzędu do Spraw Cudzoziemców lub Radzie do Spraw Uchodźców;

9) realizacji obowiązku, o którym mowa w art. 25 ust. 2 rozporządzenia (WE) nr 767/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), przysługuje konsulowi lub wojewodzie.

Art. 7. 1. Uprawnienie do pośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu wglądu do danych VIS przysługuje sądowi, prokuraturze, Policji, Straży Granicznej, Służbie Celno-Skarbowej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Ochrony Państwa, Służbie Kontrwywiadu Wojskowego, Żandarmerii Wojskowej lub Służbie Wywiadu Wojskowego, jeżeli:[3)]

1) dostęp jest konieczny w celu zapobiegania, wykrywania lub ścigania przestępstw wymienionych w art. 607w ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2018 r. poz. 1987);

2) jest to niezbędne w związku z określoną sprawą;

3) istnieją uzasadnione powody do uznania, że wgląd do danych VIS ma istotne znaczenie dla zapobiegania, wykrywania lub ścigania przestępstw, o których mowa w pkt 1.

2. Pośredni dostęp, o którym mowa w ust. 1, jest realizowany poprzez centralne punkty dostępu, którymi są odpowiednio dla:

1) sądu, prokuratury, Policji – Komendant Główny Policji;

2) Straży Granicznej – Komendant Główny Straży Granicznej;

3) Służby Celno-Skarbowej – Szef Krajowej Administracji Skarbowej;

4) Agencji Bezpieczeństwa Wewnętrznego – Szef Agencji Bezpieczeństwa Wewnętrznego;

5) Agencji Wywiadu – Szef Agencji Wywiadu;

6) Centralnego Biura Antykorupcyjnego – Szef Centralnego Biura Antykorupcyjnego;

7) (uchylony)

8)[4)] Służby Ochrony Państwa – Komendant Służby Ochrony Państwa;

9) Służby Kontrwywiadu Wojskowego – Szef Służby Kontrwywiadu Wojskowego;

10) Służby Wywiadu Wojskowego – Szef Służby Wywiadu Wojskowego;

11) Żandarmerii Wojskowej – Komendant Główny Żandarmerii Wojskowej.

Rozdział 3

Ochrona danych osobowych oraz odpowiedzialność za niezgodne z prawem działanie lub zaniechanie związane z wykorzystywaniem danych

Art. 8. 1. *Generalny Inspektor Ochrony Danych Osobowych*[5)] sprawuje kontrolę nad tym, czy wykorzystywanie danych nie narusza praw osób, których dane te dotyczą.

2. *Generalny Inspektor Ochrony Danych Osobowych*[5)] jest uprawniony do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu sprawowania kontroli, o której mowa w ust. 1.

3. Kontrola, o której mowa w ust. 1, jest sprawowana zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1)].

---

3) Wprowadzenie do wyliczenia ze zmianą wprowadzoną przez art. 315 pkt 1 ustawy, o której mowa w odnośniku 2.

4) W brzmieniu ustalonym przez art. 315 pkt 2 ustawy, o której mowa w odnośniku 2.

5) Obecnie Prezes Urzędu Ochrony Danych Osobowych na podstawie art. 166 ust. 1 ustawy, o której mowa w odnośniku 1.

Art. 9. *Generalny Inspektor Ochrony Danych Osobowych*[5)] w przypadku, o którym mowa w art. 34 ust. 4 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 w art. 49 ust. 4 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), jest organem uprawnionym do przekazania sprawy Europejskiemu Inspektorowi Ochrony Danych, w celu podjęcia działań mediacyjnych.

Art. 10. Centralny organ techniczny KSI, w zakresie wykorzystywania danych poprzez Krajowy System Informatyczny (KSI), jest administratorem danych w rozumieniu art. 7 pkt 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1)].

Art. 11. Wykorzystywanie danych może następować bez wiedzy i zgody osób, których dane dotyczą, oraz bez obowiązku ujawniania faktycznego celu zbierania danych.

Art. 12. (uchylony)

Art. 13. (uchylony)

Rozdział 4

Bezpieczeństwo Krajowego Systemu Informatycznego (KSI)

Art. 14. Organy, o których mowa w rozdziale 2, obowiązane są, w zakresie swojego działania, do współpracy z centralnym organem technicznym KSI w celu realizacji ich zadań związanych z udziałem w Systemie Informacyjnym Schengen lub Wizowym Systemie Informacyjnym, w tym do przekazywania dokumentów oraz udzielania informacji.

Art. 15. Centralny organ techniczny KSI składa ministrowi właściwemu do spraw wewnętrznych raz w roku, w terminie do dnia 31 marca, sprawozdanie z funkcjonowania Krajowego Systemu Informatycznego (KSI) w poprzednim roku kalendarzowym.

Art. 16. 1. Minister właściwy do spraw wewnętrznych sprawuje nadzór nad prawidłowością działania Krajowego Systemu Informatycznego (KSI).

2. Minister właściwy do spraw wewnętrznych, w celu wykonania nadzoru wynikającego z ust. 1, ma w szczególności prawo:

1) dostępu do wykazu zarejestrowanych przypadków, o których mowa w art. 27 ust. 1 pkt 10;

2) sprawdzania, czy Krajowy System Informatyczny (KSI) spełnia wymagania techniczne niezbędne do udziału w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym;

3) sprawdzania, czy osoby mające dostęp do Krajowego Systemu Informatycznego (KSI) zostały odpowiednio przeszkolone w zakresie bezpieczeństwa danych oraz zasad ich ochrony oraz czy posiadają upoważnienie, o którym mowa w art. 25 ust. 2, a także czy wobec tych osób przeprowadzono kontrolę bezpieczeństwa;

4) sprawdzania prawidłowości opisu zadań i funkcji osób mających dostęp do Krajowego Systemu Informatycznego (KSI);

5) sprawdzania, czy jest zapewniona odpowiednia fizyczna ochrona Krajowego Systemu Informatycznego (KSI) przez organy mające do niego bezpośredni dostęp, w szczególności czy nie ma możliwości dostępu osób nieuprawnionych do Krajowego Systemu Informatycznego (KSI).

Art. 17. 1. Minister właściwy do spraw wewnętrznych, przed uruchomieniem Krajowego Systemu Informatycznego (KSI), jest uprawniony do sprawdzenia gotowości do prawidłowej eksploatacji Krajowego Systemu Informatycznego (KSI) w ramach poszczególnych organów uprawnionych do bezpośredniego dostępu.

2. W przypadku stwierdzenia braku gotowości do prawidłowej eksploatacji Krajowego Systemu Informatycznego (KSI) w ramach poszczególnych organów uprawnionych do bezpośredniego dostępu minister właściwy do spraw wewnętrznych jest uprawniony do wstrzymania uruchomienia Krajowego Systemu Informatycznego (KSI) w ramach organu, w przypadku którego stwierdzono nieprawidłowości.

Art. 18. W przypadku stwierdzenia nieprawidłowości działania Krajowego Systemu Informatycznego (KSI) lub jego zabezpieczenia w poszczególnych organach mających do niego bezpośredni dostęp minister właściwy do spraw wewnętrznych jest uprawniony do zablokowania bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) dla organu, w przypadku którego stwierdzone zostały te nieprawidłowości, do czasu ich usunięcia.

Art. 19. W celu wykonania zadań, o których mowa w art. 16–18, minister właściwy do spraw wewnętrznych może:

1) żądać przedłożenia informacji w zakresie niezbędnym do ustalenia stanu faktycznego;

2) przeprowadzać, w godzinach urzędowania danego organu, oględziny urządzeń, nośników oraz systemów informatycznych włączonych do Krajowego Systemu Informatycznego (KSI) w ramach danego organu;

3) zlecać sporządzanie ekspertyz i opinii;

4) żądać zablokowania bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) do czasu usunięcia stwierdzonych nieprawidłowości.

Art. 20. W przypadku stwierdzenia nieprawidłowości działania Krajowego Systemu Informatycznego (KSI) minister właściwy do spraw wewnętrznych może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień i poinformowania tych osób, w określonym terminie, o wynikach tego postępowania i podjętych działaniach.

Art. 21. 1. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, techniczne warunki, sposób i tryb dokonywania wpisów danych SIS, a także związane z tym obowiązki uprawnionych organów oraz sposób i tryb aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny (KSI), mając na względzie prawidłowe wykonywanie przez Rzeczpospolitą Polską zobowiązań wynikających z udziału w Systemie Informacyjnym Schengen.

2. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób wykorzystywania Krajowego Systemu Informatycznego (KSI) jako krajowego interfejsu Wizowego Systemu Informacyjnego, w tym sposób dokonywania wpisów danych VIS, a także wglądu do danych VIS, mając na względzie prawidłowe wykonanie przez Rzeczpospolitą Polską zobowiązań wynikających z udziału w Wizowym Systemie Informacyjnym.

Art. 22. 1. Organy uprawnione zgodnie z art. 3 ust. 2 do dokonania wpisu danych SIS za pośrednictwem centralnego organu technicznego KSI kierują wniosek o dokonanie wnioskowanego wpisu danych SIS na wypełnionej karcie wpisu. Centralny organ techniczny KSI niezwłocznie dokonuje wpisu danych SIS, informując o tym organ, który wystąpił z takim wnioskiem, albo informuje organ o braku możliwości dokonania danego wpisu danych SIS oraz jego przyczynach.

2. Organy wskazane w art. 4 ust. 2 kierują zapytanie o dane SIS, do których mają dostęp pośredni, do centralnego organu technicznego KSI na wypełnionej karcie zapytania. Centralny organ techniczny KSI przekazuje niezwłocznie odpowiednie dane SIS organowi składającemu zapytanie.

3. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, wzór karty wpisu, o której mowa w ust. 1, oraz wzór karty zapytania, o której mowa w ust. 2, a także sposób ich wypełnienia, uwzględniając zakres uprawnień organów do wykorzystywania danych SIS.

Art. 23. 1. W przypadku stwierdzenia przez organ, który dokonał wpisu danych SIS, że zawarte we wpisie dane SIS są nieprawidłowe, organ ten niezwłocznie dokonuje niezbędnej modyfikacji tych danych, zawiadamiając jednocześnie o tym fakcie centralny organ techniczny KSI.

2. W przypadku stwierdzenia przez organ, który dokonał wpisu danych SIS, że upłynął okres konieczny do osiągnięcia celów, dla których wpis został dokonany, lub jest brak podstaw prawnych do dalszego przechowywania tych danych SIS albo że nie upłynął okres konieczny do osiągnięcia celów, dla których dany wpis został dokonany, organ ten odpowiednio usuwa dane SIS albo przedłuża termin przechowywania danych SIS, zawiadamiając jednocześnie o tym fakcie centralny organ techniczny KSI.

3. Centralny organ techniczny KSI informuje organy, które zgłosiły zapytanie o dane SIS, o dokonanej modyfikacji danych SIS.

4. Organy, o których mowa w art. 3 i 4, w przypadku stwierdzenia, że wykorzystywane przez te organy dane SIS są nieprawidłowe, niezwłocznie informują o tym biuro SIRENE w celu weryfikacji prawidłowości tych danych SIS.

Art. 24. Organ uprawniony do wykorzystywania danych poprzez Krajowy System Informatyczny (KSI) jest obowiązany stosować odpowiednie procedury kontrolne wskazujące działania podejmowane w ramach danego organu mające na celu zapewnienie zgodności wykorzystywania danych z obowiązującymi przepisami.

Art. 25. 1. Organ uprawniony do wykorzystywania danych poprzez Krajowy System Informatyczny (KSI) jest obowiązany do przeszkolenia z zakresu bezpieczeństwa i ochrony danych wszystkich osób mających dostęp do Krajowego Systemu Informatycznego (KSI).

2. Odbycie szkolenia, o którym mowa w ust. 1, jest warunkiem otrzymania upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz wykorzystywania danych.

3. Minister właściwy do spraw wewnętrznych, po zasięgnięciu opinii *Generalnego Inspektora Ochrony Danych Osobowych*[5)] określi, w drodze rozporządzenia, sposób przeprowadzania szkoleń z zakresu bezpieczeństwa i ochrony danych wykorzystywanych poprzez Krajowy System Informatyczny (KSI) oraz kwalifikacje osób uprawnionych do przeprowadzania tych szkoleń, uwzględniając konieczność zapewnienia ochrony danych.

4. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, tryb dostępu do Krajowego Systemu Informatycznego (KSI), sposób przydzielania osobom upoważnionym do dostępu osobistych i niepowtarzalnych identyfikatorów użytkownika, a także wzór upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz wykorzystywania danych, uwzględniając prawidłową realizację przez Rzeczpospolitą Polską obowiązków wynikających z udziału w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym.

Rozdział 5

Centralny organ techniczny KSI

Art. 26. 1. Organem odpowiedzialnym za system krajowy N.SIS II jest centralny organ techniczny KSI.

2. Do zadań centralnego organu technicznego KSI należy:

1) utworzenie, uruchomienie, eksploatacja techniczna oraz utrzymanie Krajowego Systemu Informatycznego (KSI);

2) zapewnienie sprawnego działania i bezpieczeństwa Systemu Informacyjnego Schengen w ramach systemu krajowego N.SIS II.

Art. 27. 1. W celu realizacji zadań, o których mowa w art. 26 ust. 2 pkt 1, centralny organ techniczny KSI jest w szczególności obowiązany do:

1) przestrzegania obowiązujących protokołów i procedur technicznych w celu zapewnienia kompatybilności Krajowego Systemu Informatycznego (KSI) z systemem centralnym SIS II oraz Centralnym Wizowym Systemem Informacyjnym;

2) zapewnienia, aby dane SIS przechowywane w kopii krajowej były, dzięki automatycznym aktualizacjom, identyczne i spójne z danymi przechowywanymi w systemie centralnym SIS II;

3) zapewnienia bezpieczeństwa Krajowego Systemu Informatycznego (KSI), w szczególności poprzez sporządzenie planów awaryjnych służących ochronie infrastruktury krytycznej;

4) sprawdzania, czy organy, które wykorzystują dane poprzez Krajowy System Informatyczny (KSI), mają prawo dostępu do danych;

5) umożliwienia organom, o których mowa w art. 5–7, wykorzystywania danych VIS poprzez Krajowy System Informatyczny (KSI) oraz udzielania tym organom niezbędnych informacji do prawidłowego wykonywania przez te organy zadań w zakresie uczestnictwa w Wizowym Systemie Informacyjnym;

6) przekazywania Komisji Europejskiej listy organów, o których mowa w art. 5–7;

7) współpracy z jednostką krajową Europolu w zakresie udzielania zgody na dostęp Europejskiego Urzędu Policji (Europol) do danych VIS;

8) zapobiegania dostępowi osób nieuprawnionych do Krajowego Systemu Informatycznego (KSI);

9) zapobiegania nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników informatycznych wykorzystywanych w Krajowym Systemie Informatycznym (KSI);

10) zapewnienia rejestrowania wszystkich przypadków, w których uzyskano dostęp do danych lub wykorzystano dane w inny sposób poprzez Krajowy System Informatyczny (KSI);

11) zapewnienia fizycznej ochrony danych wykorzystywanych poprzez Krajowy System Informatyczny (KSI);

12) zapobiegania wykorzystywaniu Krajowego Systemu Informatycznego (KSI) przez osoby nieuprawnione korzystające ze sprzętu do przekazywania danych;

13) zapewnienia możliwości późniejszej weryfikacji i stwierdzenia, które dane zostały wprowadzone poprzez Krajowy System Informatyczny (KSI) oraz kiedy i przez kogo zostały wykorzystane, a także w jakim zakresie zostały udostępnione;

14) zapobiegania nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych podczas transferu tych danych lub podczas przemieszczania nośników informatycznych w ramach Krajowego Systemu Informatycznego (KSI), w szczególności poprzez zastosowanie odpowiednich technik szyfrowania;

15) zapewnienia, aby osoby uprawnione do korzystania z Krajowego Systemu Informatycznego (KSI) miały dostęp wyłącznie do danych w zakresie zgodnym z upoważnieniami wynikającymi z przepisów ustawy.

2. W celu realizacji zadań, o których mowa w art. 26 ust. 2 pkt 2, centralny organ techniczny KSI jest w szczególności obowiązany do:

1) umożliwienia organom, o których mowa w art. 3 i 4, wykorzystywania danych SIS poprzez Krajowy System Informatyczny;

2) udzielania informacji niezbędnych do prawidłowego wykonywania zadań przez organy, o których mowa w art. 3 i 4;

3) współdziałania z organami, które są uprawnione do dokonywania wpisów danych SIS poprzez Krajowy System Informatyczny, w celu zapewnienia, aby wpisy danych SIS były zgodne z prawem oraz aby były one dokładne i aktualne;

4) sprawdzania, czy organy, które wykorzystują dane SIS poprzez Krajowy System Informatyczny, mają prawo dostępu do danych SIS;

5) sprawdzenia skuteczności środków mających na celu zapewnienie bezpieczeństwa danych SIS wykorzystywanych poprzez Krajowy System Informatyczny;

6) zapewnienia usuwania danych SIS wprowadzonych poprzez Krajowy System Informatyczny po upływie okresu, na który wpisy te zostały wprowadzone;

7) sprawdzenia zasadności przedłużenia okresu przechowywania danych SIS wprowadzonych poprzez Krajowy System Informatyczny;

8) przekazywania organowi zarządzającemu systemem centralnym SIS II wykazu organów, o których mowa w art. 3 i 4;

9) zapobiegania nieuprawnionemu wykorzystywaniu danych SIS.

Art. 28. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, szczegółowy sposób rejestrowania przypadków, o których mowa w art. 27 ust. 1 pkt 10, mając na względzie bezpieczeństwo i ochronę danych wykorzystywanych poprzez Krajowy System Informatyczny (KSI).

Art. 29. 1. Centralny organ techniczny KSI, przed uruchomieniem Krajowego Systemu Informatycznego (KSI), jest obowiązany poinformować ministra właściwego do spraw wewnętrznych o gotowości Krajowego Systemu Informatycznego (KSI) do uruchomienia.

2. Minister właściwy do spraw wewnętrznych, po uzyskaniu informacji, o której mowa w ust. 1, przeprowadza kontrolę w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 92 ust. 2 Konwencji Wykonawczej.

3. Po przeprowadzeniu kontroli, o której mowa w ust. 2, minister właściwy do spraw wewnętrznych przedstawia centralnemu organowi technicznemu KSI pisemną opinię w zakresie spełnienia przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 92 ust. 2 Konwencji Wykonawczej, a w przypadku stwierdzenia nieprawidłowości w Krajowym Systemie Informatycznym (KSI) przekazuje centralnemu organowi technicznemu KSI zalecenia pokontrolne w formie pisemnej.

Art. 30. 1. Centralny organ techniczny KSI, przed uruchomieniem Krajowego Systemu Informatycznego (KSI), jest obowiązany do wystąpienia do *Generalnego Inspektora Ochrony Danych Osobowych*[5)] z wnioskiem o przeprowadzenie kontroli w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1)] oraz w przepisach wydanych na podstawie art. 39a tej ustawy[1)].

2. Wniosek, o którym mowa w ust. 1, powinien zawierać opis środków technicznych i organizacyjnych określonych w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1)] oraz informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach, wydanych na podstawie art. 39a tej ustawy[1)].

3. Centralny organ techniczny KSI obowiązany jest współpracować z *Generalnym Inspektorem Ochrony Danych Osobowych*[5)] w celu przeprowadzenia kontroli, o której mowa w ust. 1, w szczególności udzielać informacji i wyjaśnień.

4. W celu wykonania zadań, o których mowa w ust. 1, *Generalny Inspektor Ochrony Danych Osobowych*[5)], zastępca *Generalnego Inspektora*[5)] lub upoważnieni przez niego pracownicy *Biura Generalnego Inspektora Ochrony Danych Osobowych*[6)], mają prawo:

1) wstępu, w godzinach od 6^{00} do 22^{00}, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest Krajowy System Informatyczny (KSI) i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych;

2) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego;

---

6) Obecnie Urzędu Ochrony Danych Osobowych na podstawie art. 167 ust. 1 ustawy, o której mowa w odnośniku 1.

3) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii;

4) przeprowadzania oględzin poszczególnych elementów Krajowego Systemu Informatycznego (KSI), w tym urządzeń, oprogramowania, procedur przetwarzania informacji;

5) zlecać sporządzanie ekspertyz i opinii.

5. *Generalny Inspektor Ochrony Danych Osobowych*[5)] po przeprowadzeniu kontroli, o której mowa w ust. 1, przedstawia centralnemu organowi technicznemu KSI pisemną opinię w zakresie spełnienia przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1)], a także w przepisach wydanych na podstawie art. 39a tej ustawy[1)], a w przypadku stwierdzenia nieprawidłowości w Krajowym Systemie Informatycznym (KSI) przekazuje centralnemu organowi technicznemu KSI zalecenia pokontrolne w formie pisemnej.

Art. 31. 1. W przypadku przedstawienia przez ministra właściwego do spraw wewnętrznych lub *Generalnego Inspektora Ochrony Danych Osobowych*[5)] zaleceń pokontrolnych, centralny organ techniczny KSI ma prawo zgłoszenia na piśmie umotywowanych zastrzeżeń co do przekazanych zaleceń pokontrolnych, w terminie 7 dni od dnia otrzymania zaleceń pokontrolnych.

2. W razie zgłoszenia zastrzeżeń, o których mowa w ust. 1, odpowiednio minister właściwy do spraw wewnętrznych lub *Generalny Inspektor Ochrony Danych Osobowych*[5)] może:

1) uznać zgłoszone zastrzeżenia za niezasadne i podtrzymać zalecenia pokontrolne;

2) uwzględnić zgłoszone zastrzeżenia w części, a w pozostałym zakresie podtrzymać zalecenia pokontrolne;

3) uwzględnić zgłoszone zastrzeżenia w całości i wydać pozytywną opinię.

Art. 32. W przypadku niezgłoszenia przez centralny organ techniczny KSI zastrzeżeń, jak również w przypadku nieuwzględnienia zastrzeżeń przez odpowiednio ministra właściwego do spraw wewnętrznych lub *Generalnego Inspektora Ochrony Danych Osobowych*[5)], centralny organ techniczny KSI obowiązany jest wykonać zalecenia pokontrolne, a następnie wystąpić z wnioskiem do organu, który przedstawił zalecenia pokontrolne, o przeprowadzenie kontroli, o której mowa w art. 29 ust. 2 lub art. 30 ust. 1.

Art. 33. Uruchomienie Krajowego Systemu Informatycznego (KSI) może nastąpić pod warunkiem uzyskania pozytywnych opinii, o których mowa w art. 29 ust. 3, art. 30 ust. 5 lub w art. 31 ust. 2 pkt 3.

Art. 34. 1. W przypadku dokonywania jakichkolwiek zmian w Krajowym Systemie Informatycznym (KSI) po jego uruchomieniu centralny organ techniczny KSI jest obowiązany przed wdrożeniem tych zmian do uzyskania pisemnej opinii ministra właściwego do spraw wewnętrznych w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 4 i 9 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 w art. 4 i 9 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), oraz opinii *Generalnego Inspektora Ochrony Danych Osobowych*[5)].

2. W celu wydania opinii minister właściwy do spraw wewnętrznych przeprowadza kontrolę w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów, o których mowa w ust. 1.

3. Po przeprowadzeniu kontroli minister właściwy do spraw wewnętrznych przedstawia centralnemu organowi technicznemu KSI pisemną opinię, o której mowa w ust. 1, a w przypadku stwierdzenia nieprawidłowości w Krajowym Systemie Informatycznym (KSI) przekazuje centralnemu organowi technicznemu KSI zalecenia pokontrolne w formie pisemnej. W przypadku przekazania zaleceń pokontrolnych przepis art. 31 stosuje się odpowiednio do centralnego organu technicznego KSI.

4. W przypadku niezgłoszenia przez centralny organ techniczny KSI zastrzeżeń, jak również w przypadku nieuwzględnienia zastrzeżeń przez ministra właściwego do spraw wewnętrznych, centralny organ techniczny KSI jest obowiązany wykonać zalecenia pokontrolne, a następnie wystąpić z wnioskiem do ministra właściwego do spraw wewnętrznych o przeprowadzenie kontroli, o której mowa w ust. 2.

5. Uzyskanie opinii *Generalnego Inspektora Ochrony Danych Osobowych*[5)], o której mowa w ust. 1, następuje w zakresie i w trybie określonych w art. 30–32.

Rozdział 6

Biuro SIRENE

Art. 35. 1. W ramach struktury Komendy Głównej Policji wyznacza się komórkę organizacyjną będącą biurem SIRENE, zapewniającą w szczególności wymianę informacji uzupełniających w trybie i zgodnie z zasadami określonymi w podręczniku SIRENE, o którym mowa w art. 8 ust. 4 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 w art. 8 ust. 4 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II).

2. Biuro SIRENE, w celu realizacji zadań, posiada bezpośredni dostęp do Krajowego Systemu Informatycznego (KSI).

Art. 36. Szefa biura SIRENE powołuje i odwołuje Komendant Główny Policji po uzyskaniu zgody ministra właściwego do spraw wewnętrznych.

Art. 37. 1. Organy, o których mowa w rozdziale 2, są obowiązane, w zakresie swojego działania, do współpracy z biurem SIRENE w celu realizacji jego zadań związanych z udziałem w Systemie Informacyjnym Schengen, w tym do wymiany informacji uzupełniających.

2. Obowiązek, o którym mowa w ust. 1, dotyczy w szczególności bezzwłocznego przekazywania do biura SIRENE, w związku z dokonaniem poprzez Krajowy System Informatyczny (KSI) wpisu danych SIS, kopii decyzji będących podstawą wpisu danych SIS do celów odmowy wjazdu dotyczących cudzoziemców będących członkami rodzin obywateli UE w rozumieniu art. 2 pkt 4 ustawy z dnia 14 lipca 2006 r. o wjeździe na terytorium Rzeczypospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin (Dz. U. z 2017 r. poz. 900 oraz z 2018 r. poz. 650).

Rozdział 7

Zmiany w przepisach obowiązujących

Art. 38–42. (pominięte)

Rozdział 8

Przepisy przejściowe i końcowe

Art. 43. Centralny organ techniczny KSI jest obowiązany do utworzenia oraz uruchomienia Krajowego Systemu Informatycznego (KSI) w terminie do dnia 1 września 2007 r.

Art. 44. Osoby mające dostęp do Krajowego Systemu Informatycznego (KSI) po dniu 1 czerwca 2008 r. muszą być przeszkolone w sposób określony w przepisach wydanych na podstawie art. 25 ust. 3, przez osoby posiadające kwalifikacje określone w tych przepisach.

Art. 45. (pominięty)

Art. 46. Ustawa wchodzi w życie z dniem ogłoszenia[7)], z tym że:

1) art. 5–7, art. 13 oraz art. 27 ust. 1 pkt 5–7 stosuje się zgodnie z określoną przez Komisję Europejską datą rozpoczęcia funkcjonowania Wizowego Systemu Informacyjnego w Rzeczypospolitej Polskiej;

2) (uchylony)

3) art. 41 wchodzi w życie z dniem określonym w decyzji Rady, zgodnie z art. 3 ust. 2 Aktu dotyczącego warunków przystąpienia Republiki Czeskiej, Republiki Estońskiej, Republiki Cypryjskiej, Republiki Łotewskiej, Republiki Litewskiej, Republiki Węgierskiej, Republiki Malty, Rzeczypospolitej Polskiej, Republiki Słowenii i Republiki Słowackiej oraz dostosowań w Traktatach stanowiących podstawę Unii Europejskiej z dnia 16 kwietnia 2003 r. (Dz. U. z 2004 r. poz. 864).

---

7) Ustawa została ogłoszona w dniu 14 września 2007 r.