ANNALES
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN – POLONIA

VOL. LXII, 1 SECTIO G 2015

AGNIESZKA DRAGAN

# System Informacyjny Schengen drugiej generacji jako nowoczesne rozwiązanie informatyczne

The Second Generation Schengen Information as a Modern IT Solution

## WPROWADZENIE

Strefa Schengen stanowi terytorium, na którym gwarantowany jest swobodny przepływ osób. Jest obszarem, gdzie została zniesiona kontrola graniczna na granicach wewnętrznych oraz są stosowane ściśle określone, jednolite zasady dotyczące kontroli na granicach zewnętrznych, wzoru wiz wydawanych cudzoziemcom, wzajemnej kooperacji pomiędzy służbami państw sygnatariuszy, w szczególności w zakresie współpracy policyjnej i sądowej w sprawach kryminalnych. Strefa Schengen powstała na skutek podpisania przez Francję, Niemcy, Belgię, Luksemburg i Niderlandy 14 czerwca 1985 roku Układu z Schengen[1]. Jego uszczegółowienie stanowi jednak podpisana 19 czerwca 1990 roku Konwencja Wykonawcza do Układu z Schengen[2]. KW nakłada na państwa sygnatariuszy środki kompensacyjne mające na celu wyrównanie poziomu bezpieczeństwa. Jest to związane przede wszystkim z powstaniem tzw. deficytu bezpieczeństwa na granicach wewnętrznych, zaistniałego przez zniesienie na nich kontroli[3]. Wśród najważniejszych środków kompensacyjnych należy wymienić utworzenie Systemu Informacyjnego Schengen oraz ujednolicenie polityki państw w zakresie cudzoziemców, przede wszystkim harmonizację polityki imigracyjnej, wizowej i azylowej[4].

[1] Preambuła Układu pomiędzy Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz. U. WE z dnia 22 września 2000 roku, L. 239/13), dalej jako: układ z Schengen.

[2] Konwencja Wykonawcza do Układu z Schengen (*Convention implementing the Schengen Agreement*) (Dz.U. L 239 POZ.09 z 22 września 2000 roku), dalej jako: KW, Konwencja lub Schengen II.

[3] Art. 7 KW.

[4] Art. 23 KW.

Kodyfikację całego zakresu zasad dorobku prawnego Schengen[5] stanowi Kodeks Graniczny Schengen[6]. Wskazuje on na ponadnarodowy charakter norm *acquis* Schengen.

## DEFINICJE

Istotne z perspektywy niniejszego opracowania jest wskazanie głównych definicji związanych z działaniem Systemu Informacyjnego Schengen.

Granice wewnętrzne stanowią „wspólne granice lądowe Umawiających się Stron, ich porty lotnicze przeznaczone do rejsów krajowych oraz ich porty morskie przeznaczone do regularnych połączeń promowych, wyłącznie z lub do innego portu na terytoriach Umawiających się Stron, bez zatrzymywania się w jakichkolwiek portach znajdujących się poza powyższymi terytoriami"[7].

Granice zewnętrzne oznaczają „granice lądowe i morskie Umawiających się Stron, ich porty lotnicze i morskie, jeżeli nie są one granicami wewnętrznymi"[8].

Państwo członkowskie, które dokonało wpisu to państwo członkowskie, które wprowadziło wpis do SIS II. Państwo członkowskie 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 Unii Europejskiej podjęła decyzję o niestosowaniu przepisów dorobku Schengen[9].

Biuro SIRENE udostępniające dane – biuro SIRENE państwa członkowskiego będące w posiadaniu odcisków palców lub fotografii osoby, w odniesieniu do której wpisu dokonało inne państwo członkowskie.

Wpis – wpis danych do SIS dokonywany przez uprawniony podmiot.

Trafienie (*hit*) w Systemie Informacyjnym Schengen, czyli gdy w wyniku sprawdzenia w SIS odnaleziono osoby lub przedmioty wprowadzone do systemu. W systemie SIS II trafienie następuje w przypadku, gdy użytkownik końco-

---

[5] Czyli *acquis* Schengen – dorobek prawny strefy Schengen, który został włączony do zasad prawnych UE na mocy Traktatu z Amsterdamu.

[6] Rozporządzenie (WE) nr 562/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 roku ustanawiające wspólnotowy kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (*Schengen Borders Code*) (Dz.U. WE z 13 kwietnia 2006 roku, L 105 P. 0001–0032), dalej: KGS.

[7] Art. 1 KW.

[8] Art. 2 KW.

[9] Art. 2 pkt 13 ustawy z dnia 24 sierpnia 2007 roku o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej (Dz.U. z 2007 roku, nr 165, poz. 1170 ze zm.), dalej jako: ustawa RP o SIS/VIS.

wy przeprowadza sprawdzenie, w wyniku sprawdzenia otrzymuje on informację o zagranicznym wpisie do SIS II, dane dotyczące wpisu w SIS II pasują do danych wprowadzonych na potrzeby sprawdzenia, w wyniku uzyskania trafienia został wystosowany wniosek o podjęcie dalszych działań[10].

## SYSTEM INFORMACYJNY SCHENGEN DRUGIEJ GENERACJI

Jednym z nadrzędnych instrumentów umożliwiających transgraniczną wymianę danych jest System Informacyjny Schengen[11]. Został on powołany na mocy Konwencji Wykonawczej do Układu z Schengen[12]. Zaczął obowiązywać od 26 marca 1995 roku. SIS zapewnia organom wyznaczonym przez kraje – strony porozumienia – dostęp do baz danych gromadzących wpisy dzięki zautomatyzowanej procedurze wyszukiwania.

System Informacyjny Schengen drugiej generacji[13] jest wielkoskalowym systemem informatycznym utworzonym na potrzeby rozszerzonej strefy Schengen oraz Unii Europejskiej. Funkcjonuje od 9 kwietnia 2013 roku[14]. Umożliwia przetwarzanie większej ilości danych oraz korzystanie z nowoczesnych funkcjonalności[15]. SIS II stanowi jednolity organizm informacyjny, a dowodem na to jest inkorporacja identycznych przepisów prawnych zawartych w SIS I[16]. Jego

---

[10] Załącznik decyzji wykonawczej Komisji (UE) 2015/219 z dnia 29 stycznia 2015 roku zastępujący załącznik do decyzji wykonawczej 2013/115/UE w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla systemu informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. UE z 18 lutego 2015 roku, L 44/75), s. 90 (dalej jako: załącznik decyzji wykonawczej).

[11] Czyli SIS pierwszej generacji, SIS I.

[12] S. Dubaj, A. Kuś, P. Witkowski, *Transgraniczny przepływ towarów i osób w Unii Europejskiej*, Lublin – Zamość 2011, s. 50.

[13] Decyzja Rady z dnia 7 marca 2013 roku ustalająca 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) (2013/158/UE) (Dz. U. UE L 087, 27 marca 2013 roku, P. 0010–001).

[14] Działania związane z utworzeniem SIS II ocenia się jako zbyt przedłużone, gdyż rozpoczęto je w 2007 roku. Co więcej, SIS II został przygotowany do obsługi co najmniej 30 państw. Ma również gromadzić ponad dwa razy więcej danych niż pierwsza generacja tego systemu. Założono, że wydajność SIS II ma być pięciokrotnie wyższa.

[15] *Uruchomienie systemu informacyjnego Schengen drugiej generacji (SIS II)*, www.policja.pl/portal/pol/1046/85824/Uruchomienie_Systemu_Informacyjnego_Schengen_drugiej_generacji_SIS_II.html [data dostępu: 08.04.2015].

[16] System drugiej generacji jednak opiera się na innych aktach prawnych, głównie na: 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.U. UE L 205, 7 sierpnia 2007 roku, P. 0063–0084) (dalej jako: decyzja SIS II) oraz rozporządzeniu (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.U. UE L 381, 28 grudnia 2006 roku, P. 0004–0023), dalej jako: rozporządzenie SIS II.

celem jest „zapewnienie przy wykorzystaniu informacji, przekazywanych za pośrednictwem tego Systemu, wysokiego poziomu ochrony w obszarze wolności bezpieczeństwa i sprawiedliwości Unii Europejskiej, w tym utrzymanie bezpieczeństwa publicznego oraz porządku publicznego i zagwarantowanie bezpieczeństwa na terytorium państw członkowskich”[17]. System ten zgodnie z założeniami powinien zawierać: wpisy dotyczące osób zaginionych w celu zapewnienia im bezpieczeństwa lub eliminacji zagrożeń; wpisy odnoszące się do osób, których obecność jest wymagana do celów postępowania sądowego; wpisy dotyczące osób lub przedmiotów dokonywane w celu przeprowadzania kontroli niejawnych lub kontroli szczególnych; wpisy dotyczące przedmiotów przeznaczonych do zajęcia lub wykorzystania jako dowód w postępowaniu karnym[18]. Należy zaznaczyć, iż cel SIS II jest znacznie szerszy w zestawieniu z jego pierwotnym zamysłem. Większe mają być również możliwości używania Systemu drugiej generacji z uwagi na poszerzony dostęp do niego, obejmujący Europol, Eurojust, prokuratorów krajowych, podmioty odpowiedzialne za rejestrację pojazdów, nowe kategorie danych w nim ujęte, wzajemne relacje między wpisami i platformę techniczną dzieloną wraz z Systemem Informacji Wizowej[19]. Przewiduje się, że w ten sposób SIS z narzędzia kontroli ma ulec przekształceniu w system sprawozdawczy i śledczy[20].

Samo wprowadzenie Systemu Informacyjnego Schengen drugiej generacji pozwala na unowocześnienie technologii informatycznych stosowanych w SIS I oraz SIS 1+[21]. SIS II zapewnia organom odpowiedzialnym za kontrole graniczne, policyjne oraz celne wymianę wiadomości o osobach podejrzanych o udział w poważnych przestępstwach. Zawiera także wpisy dotyczące osób zaginionych, przede wszystkim dzieci, oraz informacje o skradzionych, zagubionych lub przywłaszczonych przedmiotach, takich jak np. banknoty, samochody, furgonetki, broń palna czy dokumenty tożsamości.

Struktura techniczna SIS II obejmuje:

- system centralny („centralny SIS II”), który składa się z funkcji wsparcia technicznego („CS-SIS”), zawiera bazę danych („baza danych SIS II”) i jednolity interfejs krajowy („NI-SIS”),
- infrastrukturę łączności pomiędzy CS-SIS a NI-SIS („infrastruktura łączności”), dzięki której dane SIS II mogą być przekazywane przez przezna-

[17] Art. 1 rozporządzenia SIS II.

[18] Pkt 12 Preambuły do decyzji SIS II.

[19] System Informacji Wizowej (*Visa Information System*), dalej jako: VIS.

[20] P. Fajgielski, *Przetwarzanie i ochrona danych w Systemie Informacyjnym Schengen*, [w:] *Układ z Schengen. Szanse i zagrożenia dla transgranicznej współpracy Polski i Ukrainy*, pod red. A. Kusia, T. Sieniowa, Lublin 2007, s. 69–70.

[21] *Schengen Information System One for All*, system przejściowy funkcjonujący do czasu utworzenia SIS II; dalej jako: SIS 1+.

czoną do tego zaszyfrowaną sieć wirtualną i wymieniane między biurami SIRENE[22],

– system krajowy („N.SIS II") w każdym państwie członkowskim, który składa się z krajowych systemów danych, łączących się z centralnym SIS II; co więcej, może zawierać plik danych („kopia krajowa") zawierający pełną lub częściową kopię bazy danych SIS II (nadzór nad nim sprawuje Europejski Inspektor Ochrony Danych)[23].

Główna jednostka znajduje się w Strasburgu (Francja), natomiast rezerwowy CI-SIS, który może zapewnić wszystkie funkcje głównego systemu w przypadku jego awarii, jest ulokowany w Sankt Johann im Pongau (Austria). Koordynację nad realizacją zadań SIS przekazano wyspecjalizowanemu organowi Unii Europejskiej, jakim jest eu-Lisa[24].

Zgodnie z wymogami dotyczącymi funkcjonowania nowego sytemu każde państwo członkowskie jest odpowiedzialne za budowę, eksploatację i utrzymanie krajowego N.SIS II oraz przyłączenie swojego N.SIS II do NI-SIS[25]. NI-SIS składa się z jednego lokalnego interfejsu krajowego na każdy kraj członkowski, który scala fizycznie każde państwo z bezpieczną siecią. Ponadto zawiera urządzenia szyfrujące na użytek SIS II oraz połączenia między biurami SIRENE. Każde państwo członkowskie musi utworzyć również główny interfejs krajowy, który stanowi program zabezpieczający dostęp do CS-SIS[26]. Kraj członkowski ma także obowiązek wyznaczyć organ na szczeblu centralnym odpowiadający za N.SIS II („urząd N.SIS II"). Podmiot ten ma na celu zapewnienie sprawnego działania i bezpieczeństwa N.SIS II, umożliwiającego właściwym organom dostęp do SIS II. Państwo członkowskie przekazuje swoje wpisy przez urząd krajowego systemu. Obligatoryjne jest również utworzenie „krajowego biura SIRENE", zapewniającego wymianę wszelkich danych uzupełniających. Zajmuje się ono również koordynacją i weryfikacją jakości informacji wdrażanych do systemu oraz dysponuje dostępem do danych przetwarzanych w SIS II. Państwa członkowskie informują organ zarządzający o swoim krajowym urzędzie N.SIS II i biurze SIRENE[27]. Podmiot zarządzający ogłasza wykaz swoich urzędów i biur[28]. Aby

[22] S.I.Re.N.E. (*Supplementary Information Request at National Entries*) – wniosek o informacje uzupełniające na poziomie dostępów krajowych.

[23] Art. 4 ust. 1 rozporządzenia SIS II.

[24] *European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice* – Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi.

[25] Art. 6 decyzji SIS II.

[26] P. Wawrzyk, *Współpraca policyjna a System Informacyjny Schengen II*, Warszawa 2008, s. 114.

[27] Art. 7 decyzji SIS II.

[28] Wykaz Biur N.SIS II i krajowych biur SIRENE (2013/C 103/02) (Dz.U. UE. z 9 kwietnia 2013 roku, 2013/C 103/02). W Polsce biuro SIRENE i Zadania Biura SIRENE są realizowane przez: Sekcję Całodobowej Obsługi Międzynarodowego Przepływu Informacji w Wydziale Koordynacji

zagwarantować szybkie i sprawne przesyłanie danych, każdy kraj członkowski, tworząc własny N.SIS, dba o przestrzeganie protokołów i procedur technicznych ustalonych dla zapewnienia kompatybilności N.SIS z CS-SIS. Ponadto respektuje się zasady bezpieczeństwa przepływu danych i ich poufności[29].

Istotną kwestią wprowadzoną przez System Informacyjny Schengen II jest inkorporowanie kolejnych kategorii danych o osobach dostarczanych przez państwa do bazy. Należą do nich dane biometryczne – fotografie i odciski palców. Nowością jest pomoc w realizacji przepisów odnoszących się do ochrony interesów osób, których tożsamość uległa przywłaszczeniu, oraz wprowadzenie odsyłaczy do innych wpisów dokonywanych w ramach SIS II[30]. Dokładnie rzecz ujmując, katalog danych o osobach został rozszerzony na podstawie art. 20 decyzji SIS II o: fotografie, odciski palców, organ dokonujący wpisu, odesłanie do decyzji będącej powodem wpisu, odsyłacz lub odsyłacze do innych wpisów dokonanych w SIS II, rodzaj przestępstwa i informację, czy dana osoba jest uciekinierem.

*Novum* stanowi zamieszczenie w systemie drugiej generacji danych na temat osób poszukiwanych na podstawie europejskiego nakazu aresztowania[31] czy zastosowanie instytucji informacji uzupełniających, polegającej na tym, że we wpisach o osobach poszukiwanych w celu wykonania ekstradycji i aresztowania kraj, który jest autorem rekordu, może zamieścić dane posiłkowe. Ma możliwość w ten sposób poinformować pozostałe strony o tym, jaki organ wydał akt aresztowania lub inny dokument o równoważnym skutku, czy istnieje podlegający wykonaniu wyrok, podać kwalifikację prawną czynu, opisać okoliczności, konsekwencje przestępstwa czy też zamieścić wszelkie inne użyteczne dane[32]. Ponadto w systemie znajdują się informacje o przedmiotach określonych w art. 36 i 38 decyzji SIS II, które zostały skradzione, przywłaszczone, utracone lub unieważnione.

Podczas wprowadzania danych do systemu należy brać pod uwagę zakres danych, jakie są wpisywane przy uwzględnieniu informacji obligatoryjnych do wprowadzenia (determinujących możliwość utworzenia w SIS II) i fakultatywnych – dane wprowadza się, o ile są one osiągalne dla organu tworzącego wpis w systemie. W przypadku realizacji rejestracji danych dotyczących pojazdów silnikowych o pojemności silnika przekraczających 50 $cm^3$, przyczep i naczep o masie własnej przekraczającej 750 kg, przyczep turystycznych, obligatoryjnie wdra-

Międzynarodowej Wymiany Informacji oraz przez Wydział Koordynacji Poszukiwań Międzynarodowych Biura Międzynarodowej Współpracy Policji KG (Komenda Główna Policji, ul. Puławska 148/150, 02–624 Warszawa; www.policja.pl/pol/sirene/polskie-biuro-sirene [data dostępu: 20.04.2015]). Biuro SIRENE zostało powołane w celu uzupełniania danych przetwarzanych w SIS.

[29] Art. 9–11 rozporządzenia SIS II.

[30] Art. 20 ust. 1 pkt e, f, m rozporządzenia SIS II.

[31] *European arrest warrant*, dalej jako: ENA.

[32] A. Rogala-Lewicki, *Struktura Systemów Informacyjnych Strefy Schengen*, s. 16–17, www.fsap.pl/documents/publications/STRUKTURA_SYSTEMOW_INFORMACYJNYCH_STREFY_SCHENGEN.pdf [data dostępu: 20.04.2015].

ża się następujące dane: podstawę prawną wpisu, czynności do podjęcia, datę wygaśnięcia wpisu, kategorię pojazdu, markę, model oraz numer rejestracyjny pojazdu lub numer VIN albo numer nadwozia, podwozia lub ramy[33]. Dodatkowo w przedmiotowej kategorii można dokonać wpisu obejmującego: kraj rejestracji, kolor/kolory, ostrzeżenia, rok produkcji, zestaw oznaczeń RFID i zdjęcie[34].

Względem poszczególnych rzeczy może być wymagany różny zakres informacji podstawowych. Do danych obligatoryjnych zalicza się m.in.: rodzaj pojazdu, markę pojazdu, typ pojazdu, VIN lub numer rejestracyjny, zagrożenie związane z pojazdem i powód wpisu. Co do pozostałych przedmiotów, np. broni, będzie to jej rodzaj, numer oraz marka. Fakultatywnie można wpisać kaliber, model broni, zestaw oznaczeń RFID[35] i załączyć zdjęcie. Kolejne rodzaje przedmiotów, np. blankiety dokumentów, wydanych dokumentów tożsamości, banknotów, będą miały do obowiązkowego uzupełnienia różne pola – różny jest zakres informacyjny warunkujący utworzenie wpisu w systemie drugiej generacji. Wskazane powyżej przykładowe dane o przedmiotach zostały zdefiniowane w toku uzgodnień pomiędzy krajami członkowskimi i są fundamentalnymi zasadami określającymi śladową ilość informacji, jakie muszą zostać wprowadzone do bazy, aby było możliwe zrealizowanie celu wpisu.

Inkorporacja danych do Systemu Informacyjnego Schengen została doprecyzowana w decyzji SIS II oraz rozporządzeniu SIS II przez zdefiniowanie zasad, jakie powinny być stosowane przez państwa przy dokonywaniu wpisów do systemu. Wśród najistotniejszych aspektów związanych z umieszczaniem danych w SIS II znalazły się następujące postanowienia:

- z zastrzeżeniem informacji uzupełniających, system zawiera jedynie te kategorie danych, które są dostarczane przez państwa, a są niezbędne z punktu widzenia osiągnięcia celów ustanowionych w art. 26, 32, 34, 36 i 38 decyzji SIS II,
- o zasadności wpisu decyduje kraj członkowski w oparciu o wagę sprawy i celowość wprowadzenia danych,
- jedynie państwo, które wprowadziło wpis jest upoważnione do jego transformacji, uzupełnienia lub usunięcia,

---

[33] *Podręcznik użytkownika Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz Wizowego Systemu Informacyjnego (VIS) – aspekty prawne*, s. 35, http://bip.msw.gov.pl/bip/pelnomocnik-rzadu-ds-s/22089,Podrecznik-uzytkownika-Systemu-Informacyjnego-Schengen-drugiej-generacji-SISII-o.html [data dostępu: 17.04.2015], dalej jako: podręcznik SIS II.

[34] *Ibidem*, s. 35–36.

[35] RFID (*Radio-Frequency Identification*) to technologia stosowana do identyfikacji obiektów oraz kontroli przepływu produktów. Odczytywanie informacji ze specjalnych tagów, które przymocowuje się do przedmiotów (ale nie tylko, gdyż RFID znajduje zastosowanie także do znakowania zwierząt, a nawet ludzi), następuje drogą radiową. W zależności od rodzaju tagu zmienia się ilość informacji, które może on przechowywać oraz maksymalna odległość, z której można odczytać dane. Tagi RFID to alternatywa dla kodów kreskowych – wygodniejsza i bardziej wydajna.

– wprowadzanie danych o osobach następuje zgodnie z art. 20 decyzji SIS II, art. 20 rozporządzenia SIS II w związku z art. 23 decyzji SIS II oraz rozporządzenia SIS II[36].

Dzięki tym rozwiązaniom prawnym system może gwarantować odsyłanie wiadomości między wpisami odnoszącymi się do osoby poszukiwanej za uprowadzenie, osoby porwanej oraz pojazdu wykorzystanego do popełnienia tego przestępstwa[37].

Wytyczne wprowadzania wpisów do Systemu Informacyjnego Schengen przedstawiają się następująco[38]: do SIS można wprowadzić jedynie te dane o osobach, które zostały wymienione w art. 94 ust. 2 KW, art. 20 ust. 2 rozporządzenia SIS II oraz art. 20 ust. 3 decyzji SIS II, wprowadzenie innych danych o osobach jest niedopuszczalne. Wpis musi być wprowadzony w oparciu o zasadę proporcjonalności – wpis do SIS może być dokonany jedynie w sytuacji, gdy sprawa jest wystarczająco ważna dla wprowadzenia wpisu, a także gdy dany przypadek jest dodatkowo na tyle stosowny i odpowiedni, że uzasadnia to jego wprowadzenie do systemu. Ponadto wpis powinien zawierać przynajmniej informacje o nazwisku, imionach i pseudonimach osoby, jej płci i przyczynie wpisu, ponieważ w przeciwnym razie wprowadzenie danych do SIS nie będzie możliwe. Zawsze dane wprowadzane do Systemu Informacyjnego Schengen powinny być prawdziwe, aktualne i zgodne z prawem, w innym wypadku nie mogą być wprowadzone do SIS. Natomiast co do wpisów danych o cudzoziemcach, należy je przedstawić jedynie w celu odmowy pozwolenia na wjazd oraz wyłącznie na podstawie decyzji podjętej przez krajowe organy właściwe w sprawach wydawania decyzji odmawiającej pozwolenia na wjazd, gdy jest to uzasadnione zagrożeniem dla porządku publicznego, bezpieczeństwa publicznego lub bezpieczeństwa narodowego. Wpisy innych danych o osobach lub pojazdach, statkach wodnych, statkach powietrznych i kontenerach w celu przeprowadzania niejawnego nadzorowania lub kontroli wprowadzane są m.in.: w celach ścigania przestępstw, jeżeli dana osoba popełnia liczne i szczególnie poważne przestępstwa lub wpis może zostać wprowadzony; jeśli istnieje wyraźny dowód, że powyższe informacje są niezbędne do zapobiegania poważnym zagrożeniom stanowionym przez daną osobę lub poważnym zagrożeniom dla wewnętrznego i zewnętrznego bezpieczeństwa narodowego.

Kolejnym ważnym aspektem są warunki dokonywania wpisów dotyczących odmowy pozwolenia na wjazd lub pobyt obywateli państw trzecich, którzy mogą korzystać z prawa do swobodnego przepływu w obrębie Unii, ale podlegają środkom ograniczającym. Pierwsza kwestia obejmuje dane dotyczące obywateli państw trzecich, w stosunku do których został dokonany wpis w celu odmowy ze-

[36] Podręcznik SIS II, s. 36.

[37] S. Dubaj, *System Informacyjny Schengen – wdrożenie i perspektywy rozwoju*, [w:] *Transgraniczny przepływ towarów i osób w Unii Europejskiej*, pod red. A. Kusia, M. Kowerskiego, Lublin – Zamość 2012, s. 238.

[38] Podręcznik SIS II, s. 20–21.

zwolenia na wjazd lub pobyt – wprowadza się je na podstawie krajowego wpisu. Wynika on z decyzji podjętej na podstawie indywidualnej oceny przez właściwe państwowe organy administracyjne lub sądy zgodnie z prawem krajowym. Wpisu dokonuje się na podstawie decyzji, jeżeli istnieje uzasadnione ryzyko zagrożenia dla porządku, bezpieczeństwa publicznego lub bezpieczeństwa narodowego, jakie może zaistnieć w obecności danego obywatela państwa trzeciego na terytorium kraju członkowskiego. Dotyczy to również sytuacji, gdy cudzoziemiec został poddany środkom obejmującym deportację, odmowę pozwolenia na wjazd lub wydalenie, które nie zostały unieważnione ani zawieszone. Drugi aspekt dotyczy obywatela państwa trzeciego, któremu przysługuje prawo do swobodnego przepływu osób w obrębie UE w rozumieniu dyrektywy 2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 roku w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przepływu i pobytu na terytorium państw członkowskich. Jeżeli został dokonany wpis, państwo członkowskie, które go wykonuje, natychmiast konsultuje się przez biura SIRENE (zgodnie ze wskazówkami podręcznika SIRENE) z krajem członkowskim, które dokonało wpisu, aby bezzwłocznie podjąć decyzję co do wymaganych czynności[39]. Trzecia kwestia odnosi się do cudzoziemców, którzy podlegają środkom ograniczającym wprowadzonym zgodnie z art. 29 Traktatu o Unii Europejskiej[40]. Wpisy obejmujące takich obywateli mają uniemożliwić wjazd na terytorium państw członkowskich lub przejazd przez nie. Odnoszą się także do wykonania zakazu podróży wydanego przez Radę Bezpieczeństwa Organizacji Narodów Zjednoczonych. Dane takie zostają wprowadzane do SIS II w celu odmowy pozwolenia na wjazd lub pobyt, o ile spełnione są wymagania dotyczące jakości danych[41].

Wpisy przechowuje się przez okres konieczny dla osiągnięcia celów, dla których zostały wprowadzone. Państwo członkowskie, które wprowadziło wpis, w terminie trzech lat od daty jego dokonania w SIS II weryfikuje potrzebę jego zachowania. Po upływie tego czasu są one usuwane automatycznie poza sytuacjami, gdy kraj członkowski, który dokonał wpisu, przekazał do CS-SIS informację o przedłużeniu okresu przechowywania wpisu[42].

W kwestii ochrony danych osobowych w systemie drugiej generacji nowe przepisy prawne powielają rozwiązania przewidziane w Konwencji Wykonawczej do Układu z Schengen. Rozporządzenie odnoszące się do SIS II odsyła do dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych

[39] Art. 24–25 rozporządzenia SIS II.

[40] Zgodnie z nim: „Rada przyjmuje decyzje, które określają podejście Unii do danego problemu o charakterze geograficznym lub przedmiotowym. Państwa Członkowskie zapewniają zgodność swych polityk krajowych ze stanowiskami Unii".

[41] Art. 26 rozporządzenia SIS II.

[42] Art. 29 rozporządzenia SIS II.

osobowych i swobodnego przepływu tych danych, jak również do rozporządzenia WE 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 roku o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[43]. Co więcej, kwestie te reguluje także Karta Praw Podstawowych[44] (art. 8), art. 16 Traktatu o Funkcjonowaniu Unii Europejskiej oraz art. 39 Traktatu o Unii Europejskiej. Sytuacja w tym aspekcie jednak znacznie się skomplikowała z uwagi na fakt, iż mechanizmy ochrony danych mają bazować również na innych podstawach normatywnych[45]. Mimo tego funkcjonowanie SIS ma duże znaczenie dla ochrony danych osobowych, zwłaszcza że konieczność modernizacji SIS spowodowała jednoczesną potrzebę zapewnienia wyższego poziomu ochrony danych osobowych. Związane jest to z poszerzeniem dostępu do systemu dla Europolu, Eurojust i prokuratorów krajowych wszczynających postępowania karne z oskarżenia publicznego. Dotyczy to również wprowadzenia nowych kategorii danych osobowych i danych o przedmiotach przechowywanych w SIS, elektronicznej wersji ENA, wymiany informacji uzupełniających, a nawet odsyłaczy i linkowania pomiędzy poszukiwanym przedmiotem a potencjalnym sprawcą. Ważną zmianę w aspekcie ochrony danych osobowych stanowi koordynacja działań nadzorczych różnych organów. Model kontroli i nadzoru zastosowany w SIS obejmuje: krajowy niezależny organ nadzorczy oraz nadzorującego go Europejskiego Inspektora Ochrony Danych Osobowych[46].

Obecnie z Systemu Informacyjnego Schengen korzystają 22 państwa członkowskie Unii oraz Szwajcaria, Lichtenstein, Norwegia i Islandia. Zjednoczone Królestwo i Irlandia biorą udział we współpracy policyjnej w ramach SIS z wyłączeniem wpisów obejmujących obywateli państw sygnatariuszy figurujących w wykazie osób nieposiadających prawa wjazdu[47].

Należy zaznaczyć, iż mimo że System Informacyjny Schengen działa dopiero od dwóch lat, to już proponuje się jego reformę. Dotyczy to głównie kwestii prawnych, ale również zakresu współpracy policyjnej i sądowej, gdzie nie ma wystarczającego poziomu ochrony danych osobowych, co wielokrotnie podkreślał Europejski Inspektor Danych Osobowych[48].

---

[43] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 roku o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. UE z 12 stycznia 2001 roku, L 8).

[44] Karta Praw Podstawowych Unii Europejskiej (Dz.U. UE z 30 marca 2010 roku, C 83/389).

[45] P. Fajgielski, *op. cit*., s. 60.

[46] A. Grzelak, *Zarządzanie granicami w strefie Schengen*, [w:] *Wpływ acquis communautaire i acquis Schengen na prawo polskie – doświadczenia i perspektywy. 15 lat acquis Schengen w prawie Unii Europejskiej*, pod red. A. Kusia, A. Szachoń-Pszenny, t. 2, Lublin 2014, s. 131–132.

[47] S. Dubaj, *System Informacyjny Schengen…*, s. 237.

[48] A. Grzelak, *op. cit*., s. 132–133.

## KRAJOWY SYSTEM INFORMATYCZNY

Aby System Informacyjny Schengen drugiej generacji sprawnie funkcjonował, państwa członkowskie muszą podjąć wszelkie należyte środki w celu zapewnienia bezpieczeństwa podczas przekazywania danych, w tym kontroli dostępu do infrastruktury, nośników danych, przechowywania i użytkowania danych, wprowadzanych informacji oraz autokontroli[49]. W przypadku Polski całokształt problematyki odnoszącej się do dostępu do Systemu Informacyjnego Schengen (w tym SIS II) reguluje rozporządzenie Ministra Spraw Wewnętrznych z dnia 3 kwietnia 2013 roku w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny[50], ustawa z dnia 24 sierpnia 2007 roku o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej i rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 grudnia 2007 roku w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny[51].

Krajowy System Informatyczny to zespół współpracujących ze sobą urządzeń, procedur przekazywania informacji, narzędzi programowych zastosowanych w celu przetwarzania danych i infrastruktura telekomunikacyjna. Umożliwia on organom administracji publicznej czy organom wymiaru sprawiedliwości wykorzystywanie danych gromadzonych w Systemie Informacyjnym Schengen i w Wizowym Systemie Informacyjnym[52]. Krajowy System wspomaga SIS II przez wykrywanie, zapobieganie i zwalczanie wszelkich przestępstw o charakterze międzynarodowym dzięki spójnemu działaniu takich służb, jak: Straż Graniczna[53], Służba Celna[54], Policja, Żandarmeria Wojskowa, Agencja Bezpieczeństwa Wewnętrznego, Prokuratura, sądy. SC, SG i Policja przez kooperację z Systemem Informacji Schengen drugiej generacji wymieniają się informacjami o poszukiwanych przestępcach i osobach, które nie mają prawa wjazdu do strefy Schengen lub pobytu w niej, dzięki czemu jeszcze skuteczniej chronią wschodnią zewnętrzną granicę UE. Należy podkreślić, że polskie organy, które są uprawnione do dokonywania wpisów danych do Systemu Informacyjnego Schengen, mogą do SIS wpisać dane polskiego obywatela, np.

---

[49] Art. 10 ust. 1 decyzji SIS II.

[50] Rozporządzenie Ministra Spraw Wewnętrznych z dnia 3 kwietnia 2013 roku w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny (Dz.U. z dnia 5 kwietnia 2013 roku, Dz.U.2013.426), dalej jako: rozporządzenie KSI.

[51] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 grudnia 2007 roku w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny (Dz.U.2007.236.1743).

[52] Art. 2 pkt 11 ustawy RP o SIS/VIS.

[53] Dalej jako: SG.

[54] Dalej jako: SC.

na podstawie ENA wydanego przez polski wymiar sprawiedliwości lub na wniosek właściwych organów sądowych w przypadku osób wezwanych do stawienia się przed sądem w charakterze świadków[55].

W celu zapewnienia bezpieczeństwa polski system współpracuje przede wszystkim z krajowym biurem SIRENE[56], jak również z innymi służbami[57]. Zadaniem SIRENE jest opracowywanie i wdrażanie zasad współpracy podmiotów uprawnionych w zakresie użytkowania SIS II. Ustanowienie biura SIRENE w Komendzie Głównej Policji zostało dokonane w celach praktycznych, ponieważ to Policja prowadzi m.in. współpracę z międzynarodowymi podmiotami zajmującymi się zwalczaniem przestępczości. Kontrolę nad funkcjonowaniem komponentów krajowych sprawuje Generalny Inspektor Ochrony Danych Osobowych[58].

Tryb dostępu do Krajowego Systemu Informatycznego określa rozporządzenie KSI wydane na podstawie delegacji ustawowej zawartej w art. 25 ust. 4 ustawy RP o SIS/VIS. Ten akt prawny definiuje następujące rodzaje użytkowników uprawnionych do dostępu do KSI w celu wykorzystania danych SIS:

a) organ lub służba uprawniona do dostępu do KSI na podstawie ustawy RP o SIS/VIS,
b) użytkownik indywidualny – osoba fizyczna uprawniona w ramach organu lub służby do wykorzystywania danych przez KSI, która w celu dostępu do:
   – danych SIS korzysta bezpośrednio z GUI SISOne4ALL[59],
   – danych SIS korzysta bezpośrednio z aplikacji WWW SIS/WWW VIS[60],
c) użytkownik instytucjonalny – organ lub służba uprawniony do współpracy z KSI za pośrednictwem własnego systemu teleinformatycznego,
d) użytkownik końcowy – osoba fizyczna upoważniona do wykorzystywania danych przez Krajowy System Informatyczny za pośrednictwem systemu informatycznego użytkownika instytucjonalnego[61].

---

[55] *FAQ – najczęściej zadawane pytania*, www.policja.pl/pol/sirene/faq/12548,FAQ-najczesciej-zadawane-pytania.html [data dostępu: 17.04.2015].

[56] W Polsce biuro SIRENE funkcjonuje od 10 września 2007 roku. Służba dyżurna Biura SIRENE PL pełniona jest wraz z funkcjonariuszami Straży Granicznej, w ścisłej współpracy z oficerami Interpolu i EUROPOLU-u. Biura SIRENE są właściwe w zakresie wymiany informacji uzupełniających do wpisów wprowadzanych do Systemu Informacyjnego Schengen.

57 W. Pieter, *System Informacyjny Schengen – rola biura SIRENE*, [w:] *Polska w strefie Schengen. Refleksje po pierwszym roku członkostwa*, pod red. B. Radzikowskiej-Kryńczak, A. Sadownika, Warszawa 2008, s. 53–54.

[58] Art. 30 ust. 1 ustawy RP o SIS/VIS.

[59] GUI SISOne4ALL (*Graphical User Interface*) – to sposób prezentacji graficznej informacji oraz interakcji z użytkownikiem.

[60] Aplikacja WWW SIS to graficzny interfejs użytkownika KSI, wykorzystywany do aktualizowania, usuwania i wyszukiwania danych SIS.

[61] § 2 rozporządzenia KSI.

Dla zachowania bezpieczeństwa systemu obowiązują zasady ochrony informacji zgodne z wymaganiami Unii Europejskiej. Zobowiązania narodowe w zakresie bezpieczeństwa obejmują Polski Komponent SIS, czyli system informacyjny obejmujący Centralny Węzeł Polskiego Komponentu SIS[62], użytkowników indywidualnych, sieć teleinformatyczną MSW, systemy centralne użytkowników instytucjonalnych, w tym sieci teleinformatyczne i stacje dostępowe wraz z użytkownikami końcowymi, oraz infrastrukturę teleinformatyczną polskiego Biura SIRENE, Biura SIS i VIS, włączając w to ich wzajemne relacje. Polski Komponent SIS jest rozumiany jako całość infrastruktury technicznej, prawnej i organizacyjnej wraz z niezbędnym personelem uczestniczącym w wymianie informacji z centralną jednostką SIS (realizowanym jako moduł krajowy). Zobowiązania narodowe obejmowały najpierw etap SIS 1+, a aktualnie SIS II i VIS, określając uprawnienia osób funkcyjnych oraz użytkowników końcowych (instytucjonalnych i indywidualnych)[63].

Zgodnie z trybem przewidzianym w rozporządzeniu KSI w celu otrzymania dostępu do tego systemu użytkownik instytucjonalny występuje do centralnego organu technicznego KSI o wydanie certyfikatu uwierzytelniającego jego system teleinformatyczny oraz o przekazanie opisu interfejsu. Ponadto zestawia bezpieczne połączenie z wykorzystaniem certyfikatów przy współpracy z centralnym organem technicznym KSI. Odpowiedzialny jest on również za przygotowanie własnego systemu teleinformatycznego do współpracy z Krajowym Systemem w oparciu o opis interfejsu. Następnie występuje do centralnego organu technicznego KSI o potwierdzenie poprawnej konfiguracji połączenia systemów teleinformatycznych[64]. W rozporządzeniu KSI określono tryb nadawania uprawnień dla użytkowników indywidualnych, zgodnie z którym użytkownik instytucjonalny występuje do centralnego organu technicznego Krajowego Systemu z pisemnym wnioskiem o nadanie, zmianę lub cofnięcie uprawnień do dostępu do niego dla użytkownika indywidualnego lub wydanie osobistego i niepowtarzalnego identyfikatora[65]. Wskazano również tryb cofnięcia uprawnień do dostępu do KSI dla użytkowników indywidualnych[66].

Ustawa RP o SIS/VIS w art. 4 ust. 1 wskazuje organy i służby uprawnione do bezpośredniego dostępu do KSI w celu wglądu do danych Systemu Informacyjnego Schengen. Są to:

---

[62] Centralny Węzeł Polskiego Komponentu SIS to 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.

[63] *Strefa Schengen – czyli co trzeba wiedzieć o SIS*, http://zabezpieczenia.com.pl/publicystyka/strefa-schengen-czyli-co-trzeba-wiedziec-o-sis-vis-i-esi [data dostępu: 17.04.2015].

[64] § 3 rozporządzenia KSI.

[65] § 5–6 rozporządzenia KSI.

[66] § 8 rozporządzenia KSI.

- Policja, SG, SC, Agencja Bezpieczeństwa Wewnętrznego, Żandarmeria Wojskowa, Centralne Biuro Antykorupcyjne,
- organy kontroli skarbowej, sąd, prokuratura, urzędy skarbowe,
- minister właściwy do spraw wewnętrznych,
- szef Urzędu do Spraw Cudzoziemców, wojewoda, konsul lub dyrektor urzędu morskiego,
- Biuro Ochrony Rządu, Agencja Wywiadu, Służba Wywiadu Wojskowego, Służba Kontrwywiadu Wojskowego, organy jednostek wojskowych Sił Zbrojnych Rzeczypospolitej Polskiej lub wojewoda mazowiecki,
- organy samorządowe właściwe w sprawach rejestracji pojazdów[67],
- krajowe biura SIRENE.

Centralny organ techniczny KSI nadaje uprawnienia do dostępu do systemu organom i służbom, użytkownikom instytucjonalnym oraz użytkownikom indywidualnym, natomiast uprawnienia dla użytkowników końcowych nadają we własnym zakresie uprawnione organy i służby.

Centralnym organem technicznym Krajowego Systemu Informatycznego jest Komendant Główny Policji[68], zwany także COT KSI. Do jego zadań należy utrzymanie i eksploatacja KSI oraz zapewnienie należytego działania czy bezpieczeństwa SIS w ramach modułu krajowego[69]. Podmiot ten jest przede wszystkim zobowiązany do: przestrzegania protokołów i procedur technicznych w celu zapewnienia kompatybilności Krajowego Systemu Informatycznego z jednostką centralną SIS II; zapewnienia, aby dane SIS przechowywane w kopii krajowej były, dzięki automatycznym aktualizacjom, identyczne i spójne z danymi przechowywanymi w jednostce centralnej; gwarantowania bezpieczeństwa KSI, głównie przez sporządzenie planów awaryjnych służących ochronie infrastruktury krytycznej; weryfikowania, czy organy, które wykorzystują dane przez Krajowy System Informatyczny mają do nich prawo dostępu[70].

W celu realizacji powyższych i innych zadań wskazanych w ustawie RP o SIS/VIS centralny organ techniczny jest w szczególności zobowiązany do współdziałania z organami, które są uprawnione do dokonywania wpisów danych SIS przez Krajowy System Informatyczny w celu zapewnienia, aby te wpisy były zgodne z prawem, dokładne i aktualne. Ma on obowiązek udzielenia tym podmiotom informacji niezbędnych do funkcjonowania KSI. Centralny organ jest upoważniony także do zapewnienia bezpieczeństwa danych SIS wykorzystywanych przez kra-

[67] Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych SIS dotyczących różnych kwestii znajduje się w art. 3 ustawy RP o SIS/VIS. Natomiast kwestie dotyczące organów uprawnionych do wglądu do danych SIS reguluje art. 4 ustawy o SIS/VIS.

[68] Art. 2 pkt 3 ustawy RP o SIS/VIS.

[69] Art. 26 ustawy RP o SIS/VIS.

[70] Szerzej w art. 26 ustawy RP o SIS/VIS.

jową jednostkę, do badania zasadności przedłużania okresu ich przechowywania czy zapobiegania ich nieuprawnionemu wykorzystywaniu[71].

Co więcej, na podstawie art. 10 ustawy RP o SIS/VIS, w ramach wykorzystania danych przez Krajowy System Informatyczny w zakresie SIS, COT KSI pełni rolę administratora danych w rozumieniu przepisów ustawy o ochronie danych osobowych. Takie umocowanie wskazuje, że decyduje on o celach i środkach przetwarzania danych w zakresie ich zbierania, wpisywania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania i usuwania[72]. Jednakże Komendant Główny Policji, występujący na gruncie przepisów ustawy RP o SIS/VIS jako COT KSI, nie ma uprawnień do ustalania zgodności z prawem, dokładności oraz aktualności wpisów wprowadzanych przez organy, gdyż nie ma uprawnienia wglądu do spraw i materiałów stanowiących podstawę wprowadzania informacji do SIS i VIS. Centralny organ techniczny KSI w niniejszym zakresie ma jedynie możliwość dokonania weryfikacji, czy dany wpis odpowiada wymogom wprowadzenia wiadomości, ale nie ocenie merytorycznej podstawy wpisu. Jest to zasadnicza różnica, gdyż COT KSI nie może w takim przypadku ponosić odpowiedzialności za zawartość wpisu. Związane jest to także z faktem, że modyfikację czy usunięcie wpisu do SIS może przeprowadzić organ, który go wprowadził, bez znaczenia, czy dokonał tego bezpośrednio, czy za pośrednictwem COT KSI[73].

Przepisy prawa krajowego w nieodzownym zakresie precyzują również wytyczne wymagane z punktu widzenia zapewnienia bezpieczeństwa funkcjonowania Krajowego Systemu Informatycznego. Przyjęto założenie, że narodowe podmioty uprawnione do wprowadzania i wglądu danych SIS są zobowiązane do współpracy z COT KSI w celu realizacji ich zadań związanych z udziałem w Systemie Informacyjnym Schengen, w tym do przekazywania dokumentów i udzielania niezbędnych informacji[74]. Ponadto każdy z uprawnionych organów lub służb w celu wykorzystywania danych przez KSI jest zobowiązany do stosowania odpowiednich procedur kontrolnych wskazujących podejmowane w ramach danego organu i służby działania mające na celu zapewnienie zgodności wykorzystywania danych z obowiązującymi przepisami[75]. Dodatkowo przepis art. 25 ust. 1 ustawy RP o SIS/VIS nakłada na uprawnione podmioty obowiązek przeszkolenia wszystkich osób mających dostęp do Krajowego Systemu z zakresu bezpieczeństwa i ochrony danych, który jest warunkiem otrzymania upoważnienia do dostępu do systemu.

Należy podkreślić, iż w uprawnienia kontrolne czy nadzorcze w stosunku

---

[71] Art. 27 ust. 2 ustawy RP o SIS/VIS.

[72] Art. 7 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2014.1182), dalej jako: ustawa o.d.o.

[73] Podręcznik SIS II, s. 61–62.

[74] Art. 14 ustawy RP o SIS/VIS.

[75] Art. 24 ustawy RP o SIS/VIS.

do KSI wyposażony jest także minister właściwy do spraw wewnętrznych, który sprawuje nadzór nad prawidłowością działania tego systemu[76].

W wypadku dokonywania jakichkolwiek zmian w Krajowym Systemie COT KSI jest zobowiązany do uzyskania opinii ministra właściwego do spraw wewnętrznych. Gdy zostaną stwierdzone nieprawidłowości w działaniu czy zabezpieczeniu tego systemu w ramach danej instytucji władającej bezpośrednim dostępem, minister właściwy do spraw wewnętrznych jest uprawniony do zablokowania dopuszczenia do KSI do czasu ich usunięcia[77]. Aby zagwarantować sprawną realizację zakresu kompetencji oraz powyższych zadań, przepisy krajowe wyposażyły ministra właściwego do spraw wewnętrznych w uprawnienia do żądania przedłożenia wiadomości w zakresie niezbędnym do określenia stanu faktycznego czy wstrzymania bezpośredniego dostępu do Krajowego Systemu Informatycznego do czasu usunięcia stwierdzonych nieprawidłowości. Co więcej, minister może wykonywać oględziny urządzeń, nośników i systemów informatycznych włączonych do KSI w ramach danego organu lub zlecać sporządzenie ekspertyz i opinii[78]. Uprawnienia ministra w aspekcie Krajowego Systemu Informacyjnego rozciągają się również na prawo dostępu do katalogu zarejestrowanych sytuacji wglądu i wykorzystania danych przez KSI w celu sprawdzania, czy system ten spełnia wymogi techniczne konieczne do udziału w SIS i VIS, czy osoby mające dostęp do KSI zostały należycie przeszkolone w aspekcie bezpieczeństwa danych i reguł ich ochrony oraz czy posiadają upoważnienie, a także czy wobec tych osób wykonano kontrolę bezpieczeństwa, czy zagwarantowano odpowiednią fizyczną ochronę KSI przez organy mające do niego bezpośredni dostęp, a przede wszystkim, czy nie ma możliwości dostępu osób nieuprawnionych lub w aspekcie poprawności opisu zadań i funkcji osób mających dostęp do KSI[79].

Komendant Główny Policji jest zobowiązany do składania ministrowi właściwemu do spraw wewnętrznych sprawozdania z funkcjonowania KSI w poprzednim roku kalendarzowym w terminie do dnia 31 marca[80].

Organem uprawnionym do sprawowania nadzoru nad korzystaniem z danych zgromadzonych w systemie jest także Generalny Inspektor Ochrony Danych Osobowych[81]. GIODO w danym zakresie swoje funkcje dzieli z ministrem właściwym do spraw wewnętrznych, przy czym sfera jego odpowiedzialności dotyczy kwestii ochrony informacji osobowych. Sprawuje on kontrolę, sprawdzając, czy wykorzystywanie danych, w związku z korzystaniem z wiadomości SIS i VIS, nie narusza praw osób, których dane te dotyczą. W celu właściwego wykonywania zadań kontrolnych

[76] Art. 16 ustawy RP o SIS/VIS.
[77] Podręcznik SIS II, s. 59–60.
[78] Art. 19 ustawy RP o SIS/VIS.
[79] Art. 16 ustawy RP o SIS/VIS.
[80] Podręcznik SIS II, s. 59.
[81] Generalny Inspektor Ochrony Danych Osobowych, dalej jako: GIODO.

przyznano mu uprawnienie do bezpośredniego dostępu do KSI[82]. Tymczasem zakres uprawnień realizowanych zadań jest określony w przepisach ustawy o ochronie danych osobowych. Za szkody wyrządzone przez niezgodne z prawem wykorzystywanie danych SIS odpowiada Skarb Państwa. Organem reprezentującym Skarb Państwa w sprawach odszkodowawczych jest Prokuratoria Generalna Skarbu Państwa[83].

Należy zaznaczyć, że każdej osobie przysługuje prawo do uzyskania wyczerpującej informacji o dotyczących jej danych osobowych, które przetwarza się w takich zbiorach danych, jak SIS czy KSI. W myśl art. 32 ust. 5 ustawy o.d.o. zainteresowany może skorzystać z prawa do informacji, jednak nie częściej niż raz na sześć miesięcy. Osoba, której dotyczą dane, jest uprawniona do uzyskania informacji na temat przetwarzania jej danych osobowych, czy jej dane znajdują się w systemie, od kiedy są przetwarzane, z jakiego źródła pochodzą, w jaki sposób się je udostępnia, jaki jest cel i zakres ich przetwarzania oraz w jakim zakresie i komu się je udostępnia[84]. Administrator ma obowiązek udzielić odpowiedzi na powyższe informacje w terminie 30 dni. Aby uzyskać te wiadomości, należy złożyć pisemny wniosek w języku polskim. W myśl art. 30 ustawy o ochronie danych osobowych administrator może odmówić ich udostępnienia, jeżeli spowodowałoby to ujawnienie informacji stanowiących tajemnicę państwową, zagrożenie dla obronności lub bezpieczeństwa państwa, życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego, zagrożenie dla podstawowego interesu gospodarczego lub finansowego kraju, istotne naruszenie dóbr osobistych osób, których dane te dotyczą, jak również innych osób.

Zainteresowany może także wystąpić z wnioskiem do administratora o uzupełnienie, uaktualnienie, sprostowanie, usunięcie oraz czasowe lub stałe wstrzymanie przetwarzania swoich danych. Niemniej musi on wykazać, iż dane są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są nieprzydatne do realizacji celu, dla którego zostały zebrane[85]. W ten sposób podejmowane są działania w celu zapewnienia przepustowości SIS czy KSI.

Funkcjonariusze Straży Granicznej, tak jak i Policji, w celu usprawnienia i przyspieszenia wymiany informacji uzupełniających pełnią służbę w Biurze Międzynarodowej Współpracy Policji KGP, gdzie zostali wyposażeni w bezpośredni dostęp do baz danych Straży Granicznej. Umożliwia to udzielenie szybkiej i kompleksowej odpowiedzi na zapytanie skierowane do polskiego Biura SIRENE w ramach wymiany informacji uzupełniających realizowanej przez służby policyjne[86].

---

[82] Art. 8 ustawy RP o SIS/VIS.

[83] *Strefa Schengen – czyli co trzeba wiedzieć o SIS, VIS i ESI*, http://zabezpieczenia.com.pl/publicystyka/strefa-schengen-czyli-co-trzeba-wiedziec-o-sis-vis-i-esi [data dostępu: 17.04.2015].

[84] Art. 32 ust. 1–5a ustawy o.d.o.

[85] *System Informacyjny Schengen. Przewodnik korzystania z prawa dostępu*, Wspólny Organ Nadzorczy Schengen, 2009, s. 49–51.

[86] J. Ruta, G. Wanat, *Współpraca Straży Granicznej i Policji w kontekście członkostwa w Schengen*, [w:] *Polska w strefie Schengen…*, s. 88–89.

Obecnie w ramach Biura Międzynarodowej Współpracy Policji KGP prowadzony jest cykl szkoleń „Nowe wyzwania dla użytkowników SIS związane z wdrożeniem SIS II", realizowany w ramach Norweskiego Mechanizmu Finansowego na lata 2009–2014 dla programu operacyjnego PL15 „Współpraca w obszarze Schengen oraz walka z przestępczością transgraniczną i zorganizowaną, w tym przeciwdziałanie handlowi ludźmi oraz migracjom grup przestępczych". Projekt, który jest realizowany w okresie od 1 lipca 2014 roku do 30 kwietnia 2016 roku, ma na celu wzrost wiedzy i umiejętności funkcjonariuszy oraz pracowników Policji z zakresu funkcjonowania SIS II, w tym kwestii związanych z ochroną danych osobowych, m.in. przez poznanie praktycznych aspektów korzystania z nowych funkcjonalności SIS czy też wymianę doświadczeń na arenie międzynarodowej[87].

## PODSUMOWANIE

System Informacyjny Schengen stanowi nowoczesne narzędzie informatyczne dające gwarancję bezpieczeństwa państw Unii Europejskiej i strefy Schengen. SIS to największa w Europie baza danych, w której są przetwarzane określone przepisami kategorie danych osób, jak również przedmiotów poszukiwanych oraz wprowadzanych przez państwa sygnatariuszy. SIS II ma na celu poprawę rozwiązań informacyjnych zawartych w SIS I. Jest to związane przede wszystkim ze zmieniającą się liczbą państw Unii/Schengen, a tym samym z dążeniem do poprawy jakości danych i zdolności identyfikacji osób. W tym zakresie do SIS II wdrożono nowoczesne rozwiązania technologiczne, dzięki którym mogą być wprowadzane m.in. informacje o osobach, wobec których popełniono nadużycie, wykorzystując ich tożsamość, czy też przetwarzanie obok danych alfanumerycznych również danych biometrycznych, co skutkuje sprawniejszą i dokładniejszą identyfikacją osób, przy jednoczesnym przetwarzaniu danych osobowych zgodnie z zasadami celowości i proporcjonalności.

Ważną rolę w funkcjonowaniu SIS II pełnią same państwa, które są odpowiedzialne za tworzenie i funkcjonowanie krajowych rejestrów. Bezpośrednio, już na poziomie państwa, przyczyniają się one do zapewnienia wysokiego poziomu bezpieczeństwa Unii Europejskiej/Schengen. W Polsce taką rolę pełni Krajowy System Informatyczny, działający w Komendzie Głównej Policji w Warszawie.

Można twierdzić, iż przez utworzenie platformy Schengen doszło do ograniczenia swobody przepływu osób. Dotyczy ona możliwości poruszania się, pobytu i zatrudnienia na obszarze Unii/Schengen. Jej istotnym elementem jest *acquis* Schengen obejmujący środki prawne, które służą zniesieniu kontroli na

[87] Więcej na ten temat: www.policja.pl/pol/kgp/bmwp/nmf/dokumenty/2148,Dokumenty-do-pobrania.html [data dostępu: 20.04.2015].

granicach wewnętrznych państw członkowskich i wprowadzają jednolite zasady kontroli na granicach zewnętrznych UE. Dane są wprowadzane do SIS przez uprawnione do tego podmioty i to one rzeczywiście decydują o wpisie do systemu, który powinny dokonywać tylko w uzasadnionych przypadkach, przede wszystkim w celu zapewnienia bezpieczeństwa, porządku publicznego i narodowego. Jednak ustawodawstwo unijne nie definiuje zakresu działania uprawnionych podmiotów, powołując się na uregulowania krajowe, zatem nie można precyzyjnie określić jednorodnych okoliczności do ich wykorzystywania. Należy przy tym wziąć pod uwagę, że w sytuacji objęcia osoby wpisem do SIS, jej obecność na terytorium UE/Schengen nie powoduje zagrożenia tylko z tego powodu, że osoba ta została objęta wpisem do SIS dla celów odmowy wjazdu. W tym wypadku można stwierdzić, iż dochodzi do przejawów naruszenia swobody przepływu osób.

Zastanawiająca jest rola systemu, która pierwotnie miała dotyczyć zapewnienia bezpieczeństwa, a która wskazuje na pewnego rodzaju odejście od prostego modelu wspomagającego odpowiednie organy policyjne, graniczne i celne państw sygnatariuszy na rzecz podmiotu śledczego i sądowego. Świadczy o tym np. linkowanie pomiędzy wpisami. Niewykluczone, że w niedalekiej przyszłości dojdzie do reformy prawnej systemu, w tym zostanie poszerzony katalog danych osobowych wprowadzanych do SIS, co wiąże się ze wzrostem przestępczości transgranicznej i cybernetycznej czy masowym napływem imigrantów z rejonów objętych konfliktami militarnymi. Zmiany powinny być przeprowadzone także w celu wzmocnienia ochrony danych osobowych.

Reasumując, należy podkreślić wyjątkowe znaczenie Systemu Informacyjnego Schengen drugiej generacji, które opiera się na zadaniach, jakie pełni i na zasięgu terytorialnym. Można zaryzykować stwierdzenie, iż zbudowanie takiego narzędzia informatycznego przy uwzględnieniu specyficznych, technicznych rozwiązań jego użytkowników, z poszanowaniem ich ustawodawstwa, sprawia, iż jest to jedno z największych osiągnięć Unii Europejskiej (choć nie w pełni doskonałe).

## BIBLIOGRAFIA

Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. UE L 205, 7 sierpnia 2007 roku, P. 0063–0084).

Decyzja Rady z dnia 7 marca 2013 roku ustalająca 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) (2013/158/UE) (Dz.U. UE L 087, 27 marca 2013 roku, P. 0010–001).

Dubaj S., *System Informacyjny Schengen – wdrożenie i perspektywy rozwoju*, [w:] *Transgraniczny przepływ towarów i osób w Unii Europejskiej*, pod red. A. Kusia, M. Kowerskiego, Lublin – Zamość 2012.

Dubaj S., Kuś A., Witkowski P., *Transgraniczny przepływ towarów i osób w Unii Europejskiej*, Lublin – Zamość 2011.

Dyrektywa 2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 roku w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przepływu i pobytu na terytorium państw członkowskich (Dz.U. UE z 30.04.2004 L158/77).

Fajgielski P., *Przetwarzanie i ochrona danych w Systemie Informacyjnym Schengen*, [w:] *Układ z Schengen. Szanse i zagrożenia dla transgranicznej współpracy Polski i Ukrainy*, pod red. A. Kusia, T. Sieniowa, Lublin 2007.

*FAQ – najczęściej zadawane pytania*, www.policja.pl/pol/sirene/faq/12548,FAQ-najczesciej-zadawane-pytania.html [data dostępu: 17.04.2015].

Grzelak A., *Zarządzanie granicami w strefie Schengen*, [w:] *Wpływ acquis communautaire i acquis Schengen na prawo polskie – doświadczenia i perspektywy. 15 lat acquis Schengen w prawie Unii Europejskiej*, pod red. A. Kusia, A. Szachoń-Pszenny, t. 2, Lublin 2014.

Karta Praw Podstawowych Unii Europejskiej (Dz.U. UE z 30 marca 2010 roku, C 83/389).

Konwencja Wykonawcza do Układu z Schengen (Dz.U. L 239 POZ.09 z 22 września 2000 roku).

Pieter W., *System Informacyjny Schengen – rola biura SIRENE*, [w:] *Polska w strefie Schengen. Refleksje po pierwszym roku członkostwa*, pod red. B. Radzikowskiej-Kryńczak, A. Sadownika, Warszawa 2008.

*Podręcznik użytkownika Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz Wizowego Systemu Informacyjnego (VIS) – aspekty prawne*, http://bip.msw.gov.pl/bip/pelnomocnik-rzadu-ds-s/22089,Podrecznik-uzytkownika-Systemu-Informacyjnego-Schengen-drugiej-generacji-SISII-o.html [data dostępu: 17.04.2015].

Rogala-Lewicki A., *Struktura Systemów Informacyjnych Strefy Schengen*, www.fsap.pl/documents/publications/STRUKTURA_SYSTEMOW_INFORMACYJNYCH_STREFY_SCHENGEN.pdf [data dostępu: 20.04.2015].

Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 roku o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. UE z 12 stycznia 2001 roku, L 8).

Rozporządzenie (WE) nr 562/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 roku ustanawiające wspólnotowy kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz.U. WE z 13 kwietnia 2006 roku, L 105 P. 0001–0032).

Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 roku w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. UE L 381, 28 grudnia 2006 roku, P. 0004–0023).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 grudnia 2007 roku w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny (Dz.U.2007.236.1743).

Rozporządzenie Ministra Spraw Wewnętrznych z dnia 3 kwietnia 2013 r. w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny (Dz.U. z dnia 5 kwietnia 2013 roku, Dz.U.2013.426).

Ruta J., Wanat G., *Współpraca Straży Granicznej i Policji w kontekście członkostwa w Schengen*, [w:] *Polska w strefie Schengen. Refleksje po pierwszym roku członkostwa*, pod red. B. Radzikowskiej-Kryńczak, A. Sadownika, Warszawa 2008.

*Strefa Schengen – czyli co trzeba wiedzieć o SIS*, http://zabezpieczenia.com.pl/publicystyka/strefa-schengen-czyli-co-trzeba-wiedziec-o-sis-vis-i-esi [data dostępu: 17.04.2015].

*System Informacyjny Schengen. Przewodnik korzystania z prawa dostępu*, Wspólny Organ Nadzorczy Schengen, 2009.

Układ pomiędzy Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz.U. WE z dnia 22 września 2000 roku, L. 239/13).

*Uruchomienie systemu informacyjnego Schengen drugiej generacji (SIS II)*, www.policja.pl/portal/pol/1046/85824/Uruchomienie_Systemu_Informacyjnego_Schengen_drugiej_generacji_SIS_II.html [data dostępu: 08.04.2015].
Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2014.1182).
Ustawa z dnia 24 sierpnia 2007 roku o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej (Dz.U. z 2007 roku, nr 165, poz. 1170 ze zm.).
Wawrzyk P., *Współpraca policyjna a System Informacyjny Schengen II*, Warszawa 2008.
www.bip.msw.gov.pl [data dostępu: 23.04.2015].
www.fsap.pl [data dostępu: 23.04.2015].
www.policja.pl [data dostępu: 23.04.2015].
www.policja.pl/pol/kgp/bmwp/nmf/dokumenty/2148,Dokumenty-do-pobrania.html [data dostępu: 20.04.2015].
www.policja.pl/pol/sirene/polskie-biuro-sirene [data dostępu: 20.04.2015].
www.zabezpieczenia.com.pl [data dostępu: 23.04.2015].
Wykaz Biur N.SIS II i krajowych biur SIRENE (2013/C 103/02) (Dz.U. UE. z 9 kwietnia 2013 roku, 2013/C 103/02).
Załącznik decyzji wykonawczej Komisji (UE) 2015/219 z dnia 29 stycznia 2015 roku zastępujący załącznik do decyzji wykonawczej 2013/115/UE w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla systemu informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. UE z 18 lutego 2015 roku, L 44/75).

## SUMMARY

Schengen area guarantee free migration between countries. It's a territory where upon internal border control has been canceled, but on the same time Schengen area contains strict rules within external border control. It is a result the 'security deficiency' as come into existence on the internal borders and it implemented compensatory results. One of the most important compensatory result is Schengen Information System which was created in 1995. In 2013 Schengen Information System has been transformed into Schengen Information System second generation as the result of increased of member countries connection with rise security risks. This System is the main instrument which provides cross border exchange of personal and article data which are danger for security, health and the public order. It enable access to database with registrations due to automated search procedure for member countries. Schengen Information System second generation is consist of central system and national systems for all member countries to ensure high security level for European Union and Schengen citizens.

**Keywords:** Schengen Information System; Schengen Information System second generation; Schengen Area