

IZABELA JUSTYŃSKA

Bydgoska Szkoła Wyższa

ijustynska@interia.pl

SIS II jako instrument ochrony danych osobowych w Schengen

SIS II as a data protection instrument in Schengen

STRESZCZENIE

Aby skutecznie wpłynąć na likwidację, przynajmniej częściową, deficytu bezpieczeństwa w ramach Schengen i przestrzeni wolności, bezpieczeństwa i sprawiedliwości, gdzie zniesiono granice wewnętrzne i zapewnia się swobodny przepływ osób, musi działać system informatyczny zapewniający swobodę wymiany danych osobowych w celu uzupełnienia tego deficytu bezpieczeństwa. W czasach powszechnie ograniczonego wykorzystywaniem danych zaczerpniętych z sieci i ich przetwarzaniem, a jako wyjątek dla organów ochrony bezpieczeństwa i porządku publicznego w czasach swobodnego przepływu danych w Europie i poza Europą mamy do czynienia z innymi ograniczeniami dla bezpieczeństwa. Trzeba w każdym przypadku brać pod uwagę 5. wymiar prowadzenia wojny: poza tymi związanymi z działaniami na ziemi, w powietrzu, w kosmosie, na morzu, trzeba brać pod uwagę także działania w sieci. Wielkoskalowe systemy informatyczne w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, takie jak: SIS II, VIS (Wizowy System Informacyjny) i Eurodac do porównywania odcisków palców, mają na celu zagwarantowanie bezpiecznego, swobodnego przepływu danych w celach ich dalszego przetwarzania głównie przez organy ochrony bezpieczeństwa i porządku publicznego.

Zakres danych osobowych przetwarzanych w SIS II jest zadziwiająco szeroki, zastanawiające, czy wkrótce nie będzie on przedmiotem analiz Trybunału Sprawiedliwości UE ze względu na dwie ścierające się tendencje do dominacji interesu publicznego lub interesu indywidualnego. Z jednej strony bowiem mamy interes publiczny – dobro ogólne całej Unii, jej poszczególnych państw członkowskich i obywateli UE razem wziętych, czyli poczucie bezpieczeństwa. Z drugiej strony zaś mamy interes indywidualny w postaci poszanowania prawa do prywatności i ochrony danych oso-



bowych. Ponadto niejednokrotnie Trybunał Sprawiedliwości UE stawał już w obliczu tego dylematu, czyje interesy powinny przeważać. Rozważając ten dylemat, swoją pierwotną linię orzecznictwą *in dubio pro integrationem* zastąpił nowym podejściem równoważącym przynajmniej interes ogólny UE z interesem indywidualnym, a nawet, jak wskazują autorzy dzieła *Prawa człowieka i ich ochrona* (Gronowska, Jasudowicz, Balcerzak, 2005, s. 456), o profilu bardziej *in dubio pro homine*.

Artykuł jest próbą analizy sytuacji obecnej równoważącej prawowity cel SIS II z ochroną praw jednostki. Konkluzją jest perspektywa rozwoju SIS II już jako wartości dodanej w UE i Schengen.

ABSTRACT

In order to effectively fight with security deficit within Schengen and the area of freedom, security and justice without internal borders and where the freedom of movement of persons is applied the adequate informatics system must operate. It should guarantee the freedom of movement of personal data. At times when the personal data from the web is being used notoriously and it is being processed, besides at times of free movement of such a data as an exception for the public security and order institutions in Europe and beyond we have different limits for security. In each case the actions undertaken within the web must be taken into consideration apart from the actions at land, in the air, in the cosmos, at sea as a possible threat to security. The multiscale informatics systems within the area of freedom, security and justice, such as: SIS II, VIS, Eurodac are aiming at facilitating secure and free movement of personal data which is later to be processed by the institutions for the protection of public security and order. The scope of the personal data processed within SIS II is surprisingly bad and it is thought-provoking whether soon it won't be analyzed by the ECJ. There are two competing tendencies to fight for domination: in public interest and in the individual interest. On one hand we have the public interest-the wellbeing of all of the Union, it's member states, as well as the EU Citizens as a society and it is a sensation of security. On the other hand we have the individual interest: the right to respect private life and the protection of personal data. Many times the ECJ was dealing with a dilemma who's interest should prevail. Answering the dilemma, it's prior adjudication direction in *dubio pro integrationem* was changed to a new approach. This new tendency equals the public and individual interests or even is of totally opposite profile in *dubio pro homine*. This article aims to be a thorough analysis of the current situation in which the interests are being weighted: the lawful objectives of the SIS II and the protection of the rights of the individual. Concluding remarks include the perspective for development of the SIS II as in plus value in the EU and Schengen.

SŁOWA KLUCZOWE: bezpieczeństwo, Schengen, SIS II, rozporządzenie SIS II, decyzja SIS II, dane osobowe.

KEYWORDS: security, Schengen, Schengen Information System II, SIS II Regulation, SIS II Decision, personal data.



Strefa Schengen i regulacja prawna SIS II

Do Schengen należy łącznie 26 państw, w tym 22 z 28 państw UE i 4 państwa spoza UE, takie jak Norwegia, Islandia, Szwajcaria i Liechtenstein. Mimo to regulacje dotyczące bezpieczeństwa w Schengen i cały dorobek Schengen od 1999 r. (wraz z wejściem w życie traktatu amsterdamskiego) zostały zintegrowane i są rozwijane w ramach dorobku prawnego UE.

System Informacyjny Schengen ustanowiony został jako środek uzupełniająco/kompensacyjny związany z generalną zasadą, że kontrola na granicach wewnętrznych państw Schengen została zniesiona (tak stanowi Traktat o funkcjonowaniu UE w jego art. 67 pkt 2, który wszedł w życie w 2009 r.). Miał on przyczynić się do utrzymania wysokiego poziomu bezpieczeństwa w tzw. przestrzeni wolności, bezpieczeństwa i sprawiedliwości UE (tytuł V części trzeciej Polityki i działania wewnętrzne UE w Traktacie o funkcjonowaniu UE z 2007 r., wersja skonsolidowana z 2012 r.) przez wspomaganie współpracy operacyjnej organów policji i organów sądowniczych w sprawach karnych. Ustanowiony został na podstawie konwencji wykonawczej z 1990 r. do układu z Schengen z 14.6.1985 r. Wraz z jego rozszerzoną wersją – SIS 1+ stanowił zasadniczy instrument stosowania postanowień dorobku Schengen. Na mocy rozporządzenia i decyzji jeszcze wówczas Wspólnoty Europejskiej z 2001 r. utworzenie z kolei Systemu Informacyjnego Schengen drugiej generacji powierzono Komisji, tak aby sprostać wymogom funkcjonalności po przystąpieniu do UE nowych państw członkowskich (następne przystąpienia były w latach 2004, 2007 i 2013, łącznie 13 państw przystąpiło w tych latach do akcesji).

Podstawy prawne niezbędne dla z kolei Systemu Informacyjnego Schengen drugiej generacji stanowią takie akty instytucji unijnych, jak:

- ▶ rozporządzenie wówczas jeszcze Wspólnoty Europejskiej nr 1987/2006 z 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) – w kwestiach objętych zakresem stosowania TWE – szczególnie tytułem IV części trzeciej tego traktatu, dalej rozporządzenie SIS II, oraz
- ▶ decyzja Rady, wówczas jeszcze WE 2007/533/WsiSW, z 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) – w kwestiach objętych zakresem stosowania TUE – szczególnie w kwestiach objętych tytułem VI TUE, dalej decyzja SIS II.



System ten rozpoczął funkcjonowanie 9 kwietnia 2013 r. W tym czasie przyjmowano instrumenty prawne pozwalające na ewolucję w związku z powstawaniem SIS II, np. rozporządzenie UE Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z 25 października 2011 r. ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, które ustanowiło organ zarządzający (§ 4 preambuły do tego rozporządzenia).

Mimo odrębnych aktów jako podstawy prawnej SIS II stanowi on i powinien funkcjonować jako jednolity system informacyjny, stąd niektóre postanowienia zasadniczych aktów są identyczne (§ 4 preambuły do rozporządzenia SIS II).

SIS II wprowadzony został we wszystkich państwach członkowskich UE, z wyjątkiem Chorwacji, Cypru i Irlandii, a także w czterech państwach spoza UE: Islandii, Norwegii, Szwajcarii i Liechtensteinie. W Bułgarii i Rumunii stosuje się SIS II, mimo że utrzymano tam granice wewnętrzne. Natomiast Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej ma dostęp do SIS II, ale w ograniczonym zakresie, tzn. z wyjątkiem wpisów dokonywanych w związku z odmową pozwolenia na wjazd na terytorium Schengen.

Cel SIS II

Celem SIS II jest (zgodnie z rozporządzeniem SIS II art. 1 i art. 1 decyzji SIS II z 2007 r.) zapewnienie przy korzystaniu z informacji przekazywanych za pośrednictwem tego systemu wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości UE, w tym:

- ▶ po pierwsze, utrzymywanie bezpieczeństwa publicznego oraz porządku publicznego,
- ▶ po drugie, zagwarantowanie bezpieczeństwa na terytorium państw członkowskich,
- ▶ po trzecie, stosowanie postanowień TFUE (tytułu IV i V części III) odnoszących się do przepływu osób na terytorium państw członkowskich oraz przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

Miałyby to skutecznie/efektywnie wpłynąć na likwidację przynajmniej częściową deficytu bezpieczeństwa w ramach Schengen i przestrzeni wolności, bezpieczeństwa i sprawiedliwości, gdzie zniesiono granice wewnętrzne i zapewnia się swobodny przepływ osób.



SIS II jest systemem informacyjnym umożliwiającym krajowym organom ścigania, sądowym i administracyjnym, wykonywanie określonych zadań przez wymianę istotnych danych. Ograniczone prawa dostępu do systemu mają również europejskie agencje EUROPOL (Europejski Urząd Policji) i EUROJUST (Europejska Jednostka Współpracy Sądowej).

W związku z tą rolą SIS II system ten zawiera wpisy dotyczące osób i przedmiotów podlegające specjalnym kategoriom. Dane osobowe są w efekcie przetwarzane w SIS II.

Rodzaje danych i cele ich przetwarzania w SIS II

Moją intencją jest analiza, jakiego rodzaju dane osobowe i dla jakich celów są przetwarzane w SIS II. SIS II zawiera wpisy dotyczące osób lub przedmiotów, ja skoncentruję się na wpisach dotyczących osób, które podlegają następującym kategoriom:

- ▶ odmowa pozwolenia na wjazd lub pobyt (art. 24 rozporządzenia SIS II) – wpisy te dotyczą obywateli państw trzecich, którzy nie są uprawnieni do wjazdu bądź pobytu na terytorium strefy Schengen; osoby poszukiwane w celu aresztowania (art. 26 decyzji SIS II) – wpisy te dotyczą osób, wobec których wydano Europejski Nakaz Aresztowania lub wnioski ws. ekstradycji; osoby zaginione (art. 32 decyzji SIS II) – celem tych wpisów jest odnalezienie osób zaginionych, w tym dzieci, i objęcie ich odpowiednią ochroną, jeśli jest to konieczne; osoby, których obecność jest wymagana do celów procedury sądowej (art. 34 decyzji SIS II) – celem tych wpisów jest ustalenie miejsca zamieszkania lub pobytu osób, których obecność jest wymagana do celów procedury sądowej, np. świadków lub osób, którym ma zostać doręczony wezwanie do stawienia się w celu odbycia kary pozbawienia wolności; osoby lub przedmioty wprowadzane w celu przeprowadzania kontroli niejawnych lub kontroli szczególnych (art. 36 decyzji SIS II) – celem tych wpisów jest uzyskanie informacji o osobach lub przedmiotach w celu ścigania przestępstw oraz zapobiegania zagrożeniom bezpieczeństwa publicznego lub narodowego.

Zgodnie z art. 20 decyzji SIS II i art. 20 rozporządzenia SIS II informacje o osobach, w odniesieniu do których dokonano wpisu, nie zawierają innych danych niż:

- imię i nazwisko, pseudonimy;
- wszelkie szczególne, obiektywne cechy fizyczne niepodlegające zmianom;



- miejsce i data urodzenia;
- płeć;
- fotografie;
- odciski palców;
- obywatelstwo;
- informacja, czy dana osoba jest uzbrojona, agresywna lub czy jest uciekinierem;
- powód wpisu;
- organ dokonujący wpisu;
- odesłanie do decyzji będącej powodem wpisu;
- działania, jakie należy podjąć;
- odsyłacz do innych wpisów dokonanych w SIS II;
- rodzaj przestępstwa.

Tak też SIS II zawiera informacje, które są wystarczające na potrzeby zidentyfikowania osoby lub też przedmiotu oraz podjęcia koniecznych działań, ale państwa członkowskie przekazują sobie również informacje uzupełniające dotyczące dokonywanych wpisów, tak aby funkcjonowanie SIS II było skuteczne/efektywne. W tym zakresie niezbędne jest wskazanie na podstawowy obecnie obowiązujący akt w tej sferze, którym jest decyzja wykonawcza Komisji (UE) 2015/219 z 29 stycznia 2015 r. zastępująca załącznik do decyzji wykonawczej 2013/115/UE w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla systemu informacyjnego Schengen drugiej generacji (SIS II), ponieważ wymiana informacji uzupełniających odbywa się za pośrednictwem biur SIRENE.

Każde państwo będące stroną konwencji wykonawczej z 1990 r. do układu z Schengen z 1985 r. na podstawie art. 108 tej konwencji powołuje organ zwany biurem SIRENE (skrót od nazwy: Supplementary Information REquest at the National Entries) jako organ odpowiedzialny za moduł krajowy SIS obecnie drugiej generacji. Dnia 9 sierpnia 2004 r. zapadła decyzja ministra spraw wewnętrznych i administracji i powierzono zadania związanych z organizacją i działaniem polskiej komórki SIRENE – Policji (KGP). We wrześniu 2007 r. przeprowadzono misję ewaluacyjną. Grupa ekspertów z UE oceniała stan przygotowań polskiej Policji do wejścia do strefy Schengen i polskie biuro SIRENE zostało pozytywnie ocenione. Następnie w grudniu 2007 r. zniesiono kontrolę



na granicach lądowych, a w marcu 2008 r. zniesiono kontrolę na granicach powietrznych, natomiast 15 maja 2008 r. utworzone zostało Biuro Międzynarodowej Współpracy Policji KGP.

Ponadto w myśl polskiej ustawy z 24 sierpnia 2007 r. o udziale RP w SIS oraz systemie informacji wizowej w Polsce administratorem danych przetwarzanych w systemie informacyjnym Schengen jest Komendant Główny Policji. Do niego należy zgłaszać wnioski o udostępnienie lub modyfikację danych.

Zgodnie z art. 36 tej samej ustawy z 2007 r. szefa biura SIRENE powołuje i odwołuje Komendant Główny Policji po uzyskaniu zgody ministra właściwego do spraw wewnętrznych. W dniu 21 września 2017 roku Komendant Główny Policji powołał pana mł. insp. Tomasza Kwiatkowskiego, Naczelnika Wydziału Koordynacji Poszukiwań Międzynarodowych Biura Międzynarodowej Współpracy Policji KGP, na szefa polskiego Biura SIRENE. Jeśli chodzi o biura SIRENE, to w swoich działaniach powinny one kierować się Podręcznikiem SIRENE (SIRENE Manual). Jest to zbiór procedur opisujących szczegółowe zasady wymiany informacji uzupełniających, określa ogólne procedury SIRENE, określa szczegółowe procedury dla poszczególnych kategorii wpisów.

W związku z tym niezbędne jest, żeby podkreślić, że Komisja Europejska na początku 2015 r. zmieniła swoją decyzję z 2013 r., zastępując dotychczasowy podręcznik SIRENE, tak aby odzwierciedlał on nowe wyzwania i wymogi operacyjne oraz aby zawarte w nim przepisy w niektórych obszarach związanych z przetwarzaniem danych SIS II były bardziej precyzyjne. Stwierdzono, że powinno to zwiększyć pewność prawa i zapewnić dalsze wzmocnienie praw podstawowych, a dokonano tego po konsultacji z Europejskim Inspektorem Ochrony Danych.

Dostęp do danych w SIS II i prawa podmiotu danych osobowych

SIS II zapewnia wymianę informacji między służbami odpowiedzialnymi za:

- ochronę granic,
- wydawanie wiz,
- bezpieczeństwo publiczne.

Stąd w Polsce instytucjami uprawnionymi do korzystania z SIS II, które mają w związku z tym różny zakres uprawnień, są: minister spraw wewnętrznych i administracji, prezes Urzędu ds. Repatriacji, wojewoda, policja, straż graniczna,



minister sprawiedliwości, sąd, prokurator, służby celne, Generalny Inspektor Informacji Finansowej, Generalny Inspektor Kontroli Skarbowej, Agencja Bezpieczeństwa Wewnętrznego, minister spraw zagranicznych oraz konsul. Wynika to z ustawy z 2007 r. o udziale RP w SIS oraz Systemie Informacji Wizowej.

Należy mieć na uwadze, że wykorzystywanie danych systemu SIS może następować bez wiedzy i zgody osób, których dane dotyczą, oraz bez obowiązku ujawniania faktycznego celu zbierania danych. Aby zapewnić odpowiednią ochronę prawną osób, których dane są przechowywane w systemie SIS, Generalny Inspektor Ochrony Danych Osobowych sprawuje kontrolę nad tym, czy wykorzystywanie danych nie narusza praw osób, których dane te dotyczą. Kontrola ta jest sprawowana zgodnie z przepisami ustawy z 1997 r. o ochronie danych osobowych. Każda osoba, której dane są przetwarzane w SIS II, ma prawo wnieść skargę do Generalnego Inspektora Ochrony Danych Osobowych na wykonywanie przepisów 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.

Stąd osobom, których dane osobowe są gromadzone, przechowywane lub w inny sposób przetwarzane w SIS II, przysługuje prawo dostępu do danych, korekty nieścisłości oraz usunięcia danych wprowadzonych niezgodnie z prawem.

Tak też osobom, których dane są przetwarzane w systemie SIS II, przysługują następujące prawa wynikające z rozporządzenia SIS II i decyzji SIS II:

- prawo do dostępu do danych;
- prawo do poprawienia lub usunięcia danych;
- prawo do złożenia skargi do organu ochrony danych osobowych lub do sądu.

Każdy, kto korzysta z dowolnego z tych praw, może złożyć wniosek do właściwego organu w wybranym przez siebie państwie, niezależnie od państwa członkowskiego, w którym dokonano wpisu do SIS II.

Każda osoba, której dane dotyczą, na podstawie art. 41 rozporządzenia SIS II i art. 58 decyzji SIS II ma prawo dostępu do dotyczących jej danych, przetwarzanych w SIS II. Prawo dostępu jest wykonywane zgodnie z przepisami państwa członkowskiego, w którym składany jest wniosek. Procedury różnią się w zależności od kraju oraz przepisów dotyczących przekazywania danych wnioskodawcom.



W przypadku gdy dane państwo członkowskie otrzyma wniosek o dostęp do wpisu, którego samo nie dokonało, musi umożliwić państwu, które dokonało wpisu, zajęcie stanowiska w sprawie możliwości udostępnienia danych wnioskodawcy.

Zgodnie z art. 41 ust. 5 rozporządzenia SIS II i 58 ust. 5 decyzji SIS II, gdy przetwarzane dane są nieprawidłowe lub zostały przekazane niezgodnie z prawem, osoba, której dane te dotyczą, ma prawo do żądania poprawienia lub usunięcia tych danych.

Zgodnie z art. 34 ust. 2 rozporządzenia SIS II i art. 49 ust. 2 decyzji SIS II do zmiany lub usunięcia wprowadzonych danych uprawnione jest wyłącznie państwo członkowskie, które dokonało wpisu. W związku z tym, jeżeli wniosek jest składany w państwie członkowskim, które nie dokonało wpisu, wówczas zainteresowane państwa członkowskie współpracują ze sobą w celu znalezienia rozwiązania przez wymianę informacji i dokonanie odpowiednich weryfikacji.

Artykuł 43 rozporządzenia SIS II i art. 59 decyzji SIS II przewidują środki odwoławcze przysługujące osobom fizycznym w przypadku nieuwzględnienia ich wniosku. Osoba, której dane dotyczą, może wystąpić do sądów lub organów właściwych na mocy prawa krajowego dowolnego z państw członkowskich z wnioskiem o dostęp do informacji, poprawienie, usunięcie lub o odszkodowanie w związku z dotyczącym go wpisem.

Należy zastanowić się, jak wygląda realizacja tych praw w RP.

Każdej osobie przysługuje prawo do uzyskania wyczerpującej informacji o dotyczących jej danych osobowych, które przetwarza się w zbiorach danych. W myśl art. 32 ust. 5 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych z prawa do informacji można skorzystać nie częściej niż raz na 6 miesięcy. Za wnioski o dostęp nie pobiera się żadnych opłat.

Zgodnie z art. 32 ust. 1–5a ustawy o ochronie danych osobowych osoba, której dotyczą dane, ma prawo wystąpić o uzyskanie następujących informacji na temat przetwarzania jej danych osobowych:

- czy jej dane figurują w systemie;
- od kiedy przetwarza się jej dane;
- z jakiego źródła dane te pochodzą;
- w jaki sposób się je udostępnia;
- w jakim celu i zakresie są one przetwarzane;
- w jakim zakresie i komu się je udostępnia.



Administrator udziela żądanych informacji w terminie 30 dni. Aby informacje te uzyskać, należy złożyć pisemny wniosek.

W myśl art. 34 ustawy o ochronie danych osobowych administrator może odmówić ich udostępnienia, jeżeli spowodowałyby to:

- 1) ujawnienie wiadomości stanowiących tajemnicę państwową,
- 2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego,
- 3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
- 4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

Ponadto zainteresowany może wystąpić do administratora o uzupełnienie, uaktualnienie, sprostowanie, usunięcie oraz czasowe lub stałe wstrzymanie przetwarzania swoich danych. Niemniej zainteresowany musi wykazać, że dane są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są już zbędne do realizacji celu, dla którego zostały zebrane.

Perspektywy rozwoju SIS II

Warto dodać, że Komisja zaproponowała przepisy poprawiające skuteczność i sprawność operacyjną SIS II. Przygotowanie tych przepisów zapowiedziano w komunikacie z kwietnia 2016 r. dotyczącym planu działań na rzecz utworzenia skutecznej i trwałej unii bezpieczeństwa (Przywrócenie strefy Schengen – Plan działania, Bruksela 2016) oraz potwierdzono w orędziu o stanie Unii z 2016 r. przewodniczącego Junckera. SIS II jest najczęściej stosowanym systemem wymiany informacji służącym do zarządzania granicami i zapewniania bezpieczeństwa w Europie. Proponowane zmiany zwiększą zdolność systemu do zwalczania terroryzmu i przestępczości transgranicznej, usprawnią zarządzanie granicami i migracją oraz zapewnią skuteczną wymianę informacji między państwami członkowskimi w celu zwiększenia bezpieczeństwa europejskich obywateli (Dragan, 2015, s. 51).

Komisja w sprawozdaniu z oceny SIS stwierdziła, że system ten zapewnia wyraźną wartość dodaną na poziomie UE. Odniósł on wyjątkowy sukces operacyjny i techniczny. W ocenie wskazano jednak obszary, w których można wprowadzić ulepszenia techniczne i operacyjne w celu dalszego zwiększenia skuteczności systemu, którego wydajność jest w pełni zależna od jakości wprowadzanych do niego danych.



Zaproponowane przez Komisję zmiany:

- ▶ zwiększą bezpieczeństwo i dostępność systemu, zapewniając jednolite wymogi dla funkcjonariuszy w terenie dotyczące sposobu przetwarzania danych SIS w bezpieczny sposób i zapewnienia ciągłości działania dla użytkowników końcowych;
- ▶ wzmocnią ochronę danych poprzez wprowadzenie dodatkowych zabezpieczeń, aby zapewnić, że gromadzenie i przetwarzanie danych oraz dostęp do danych są ograniczone do tego, co ściśle niezbędne, z pełnym poszanowaniem prawa UE i praw podstawowych, w tym prawa do skutecznego środka odwoławczego;
- ▶ poprawią wymianę informacji i współpracę między państwami członkowskimi, zwłaszcza dzięki wprowadzeniu nowej kategorii wpisów dotyczących „nieznanych osób poszukiwanych” oraz przyznaniu Europolicy pełnego dostępu do systemu;
- ▶ pomogą zwalczać terroryzm przez wprowadzenie obowiązku dokonania wpisu w SIS w przypadkach związanych z przestępstwami terrorystycznymi oraz nowego zapytania kontrolnego, które pomoże właściwym organom w zdobyciu niezbędnych informacji;
- ▶ zwiększą ochronę dzieci, umożliwiając właściwym organom wydawanie – oprócz powiadomień dotyczących zaginionych dzieci – wpisów prewencyjnych, dotyczących dzieci, które są najbardziej zagrożone uprowadzeniem;
- ▶ przyczynią się do skutecznego egzekwowania zakazów wjazdu dla obywateli państw trzecich na granicach zewnętrznych dzięki wprowadzeniu obowiązku rejestrowania takich informacji w SIS;
- ▶ zwiększą egzekwowalność decyzji nakazujących powrót nielegalnie przebywających obywateli państw trzecich dzięki wprowadzeniu nowej kategorii wpisów dotyczących takich decyzji;
- ▶ poprawią skuteczność stosowania danych, takich jak wizerunki twarzy i odciski dłoni, do identyfikacji osób wjeżdżających do strefy Schengen.

Z pewnością więc zakres katalogu danych osobowych wprowadzanych do SIS II zostanie poszerzony i wzrośnie jeszcze rola SIS II jako instrumentu ochrony danych osobowych (Easton, 2016).



Bibliografia

- Dragan A. (2015). *System Informacyjny Schengen drugiej generacji jako nowoczesne rozwiązanie informatyczne*, „Annales Universitatis Mariae Curie-Skłodowska”, vol. LXII, 1, s. 33–53.
- Easton C. (2016). *Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification*, Short Paper-Ethical, Legal and Social Issues, Brazil.
- Gronowska B., Jasudowicz T., Balcerzak M., Lubiszewski M., Mizerski R. (2005). *Prawa człowieka i ich ochrona*, Toruń: Wyd. TNOiK, s. 456.
- Grupa Koordynująca Nadzór nad SIS II, System Informacyjny Schengen Przewodnik dotyczący korzystania z prawa dostępu, Bruksela 2015, s. 60–63.

Źródła internetowe

- European Commission, Migration and Home Affairs, Schengen Area, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen_en (dostęp: 10 listopada 2017 r.).
- Blim M., Dobosz A. (2008). *Strefa Schengen, czyli co trzeba wiedzieć o SIS, VIS I ESI*, „Zabezpieczenia”, 3/4, <http://www.zabezpieczenia.com.pl/publicystyka/strefa-schengen-czyli-co-trzeba-wiedzie%C4%87-o-sis-vis-i-esi> (dostęp: 10 listopada 2017 r.).
- Komisja Europejska, Przedstawicielstwo w Polsce, Bezpieczeństwo Schengen, https://ec.europa.eu/poland/news/161221_schengen_pl (dostęp 10 listopada 2017 r.).
- Policja.Pl, *Co to jest System Informacyjny Schengen (SIS)*, <http://www.policja.pl/pol/sirene/sis/12473,Co-to-jest-System-Informacyjny-Schengen-SIS.html> (dostęp: 10 listopada 2017 r.).
- Strzępka K. (PAP), *Zmiany w strefie Schengen Wejdzie w życie nowy system (EES)*: <http://fakty.interia.pl/swiat/news-zmiany-w-strefie-schengen-wejdzie-w-zycie-nowy-system,nld,2457435> (dostęp: 10 listopada 2017 r.).

Akty prawne

- Decyzja nr 296 Komendanta Głównego Policji z dnia 18 sierpnia 2016 r. zmieniająca decyzję w sprawie procedur postępowania w przypadku odnalezienia osoby lub przedmiotu na skutek wglądu do danych SIS, data ogłoszenia: 2016-09-01, data wejścia w życie: 2016-09-16, data obowiązywania: 2016-09-16, która zmieniła decyzję wcześniejszą nr 137 Komendanta Głównego Policji z dnia 10 kwietnia 2013 r. w sprawie procedur postępowania w przypadku odnalezienia osoby lub przedmiotu na skutek wglądu do danych SIS, na podstawie art. 5 ust. 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2015 r. poz. 355, z późn. zm. 1).
- Decyzja Rady z dnia 6 grudnia 2012 r. w sprawie wniosku Irlandii o zastosowanie wobec niej niektórych przepisów dorobku Schengen dotyczących ustanowienia Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, Dz.Urz. UE L 337/48 z 11.12.2012 r.



- Decyzja Rady 2009/426/WSiSW z dnia 16.12.2008 r. w sprawie wzmocnienia Eurojustu i w sprawie zmiany decyzji 2002/187/WSiSW ustanawiającej Eurojust w celu zintensyfikowania walki z poważną przestępczością, Dz.Urz. UE L 138/14 z 4.6.2009 r.
- 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.Urz. UE L 205/63 z 7.8.2007 r.
- Decyzja Wykonawcza Komisji z dnia 26 lutego 2013 r. w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla systemu informacyjnego Schengen drugiej generacji (SIS II), Dz.Urz. UE L 71/1 z 14.3.2013 r.
- Decyzja Wykonawcza Komisji (UE) 2015/219 z dnia 29 stycznia 2015 r. zastępująca 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.Urz. UE L 44/75 z 18.2.2015 r.
- Dyrektywa 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 uchyłająca decyzję ramową Rady 2008/977/WSiSW, Dz.Urz. UE L 119/89 z 4.5.2016 r.
- Karta Praw Podstawowych UE, Dz.Urz. UE C 326 z 26.10.2012, s. 391–407.
- Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej i Rady. Przywrócenie strefy Schengen-Plan działania, Bruksela 2016 COM (2016) 120 final z 4.3.2016 r.
- Konwencja Wykonawcza do Układu z Schengen z dnia 14.6.1985 r. z 1990 r., Dz.Urz. UE L 239 z 22.9.2000 r., s. 19–62.
- Obwieszczenie Marszałka Sejmu RP z dnia 13 czerwca 2016 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych, Dz.U. RP z 2016 r. poz. 922.
- Obwieszczenie Marszałka Sejmu RP z dnia 30.7.2014 r. w sprawie ogłoszenia jednolitego tekstu ustawy o udziale RP w SIS oraz Wizowym Systemie Informacyjnym z 24.8.2007 r., Dz.U. RP poz. 1203 z 10.9.2014 r.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/958/WSiSW, Dz.Urz. UE L 135/53 z 24.5.2016 r.
- Rozporządzenie (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 381/4 z 28.12.2006 r.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, Dz.Urz. UE L 286/1 z 1.11.2011 r.



- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływy osób przez granice (kodeks graniczny Schengen), Dz.Urz. UE L 77/1 z 23.3.2016 r.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 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 oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona), Dz.Urz. UE L 180/1 z dnia 29.6.2013 r.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/458 z dnia 15 marca 2017 r. zmieniające rozporządzenie (UE) 2016/399 w odniesieniu do zintensyfikowania odpraw na granicach zewnętrznych z wykorzystaniem odpowiednich baz danych, Dz.Urz. UE L 74/1 z dnia 18.3.2017 r.
- Rozporządzenie Rady (UE) nr 1273/2012 z dnia 20 grudnia 2012 r. w sprawie migracji z systemu informacyjnego Schengen (SIS 1+) do systemu informacyjnego Schengen drugiej generacji (SIS II) (wersja przekształcona), Dz.Urz. UE L 359/32 z dnia 29.12.2012 r.
- Sprawozdanie z dnia 21.12.2016 r. Komisji dla Parlamentu Europejskiego i Rady w sprawie oceny Systemu Informacyjnego Schengen drugiej generacji (SIS II) zgodnie z art. 24 ust. 5, art. 43 ust. 3 i art. 50 ust. 5 rozporządzenia (WE) nr 1987/2006 i art. 59 ust. 3 i art. 66 ust. 5 decyzji 2007/533/WSiSW, COM (2016) 880 final, Bruksela 2016.
- Traktat z Amsterdamu zmieniający Traktat o Unii Europejskiej, Traktaty ustanawiające Wspólnoty Europejskie i związane z nimi akty prawne z dnia 2.10.1997 r., Dz.Urz. UE C 340 z 10.11.1997, s. 1–144.
- Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie dnia 13 grudnia 2007 r., Dz.Urz. UE C 306 z 17.12.2007 r.
- Traktat o funkcjonowaniu UE, Dz.Urz. UE C 326 z 26.10.2012, s. 47–390.
- Traktat o UE, Dz.Urz. UE C 326 z 26.10.2012, s. 0001–0390.
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 1997 r. Nr 133, poz. 883.
- Ustawa z dnia 24 sierpnia 2007 r. o udziale RP w Systemie Informatycznym Schengen oraz Systemie Informacji Wizowej, Dz.U. z 2007 r. Nr 165, poz. 1170.