Rada
Unii Europejskiej

Bruksela, 23 grudnia 2016 r.
(OR. en)

15813/16

Międzyinstytucjonalny numer referencyjny:
2016/0408 (COD)

SIRIS 177
FRONT 502
SCHENGEN 21
COMIX 862
CODEC 1944

WNIOSEK

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Data otrzymania:	22 grudnia 2016 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2016) 882 final
Dotyczy:	Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmieniające rozporządzenie (UE) nr 515/2014 i uchylające rozporządzenie (WE) nr 1987/2006

Delegacje otrzymują w załączeniu dokument COM(2016) 882 final.

Zał.: COM(2016) 882 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 21.12.2016 r.
COM(2016) 882 final

2016/0408 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmieniające rozporządzenie (UE) nr 515/2014 i uchylające rozporządzenie (WE) nr 1987/2006

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

W swoich pracach prowadzonych na przestrzeni ostatnich dwóch lat Unia Europejska mierzyła się jednocześnie z odrębnymi wyzwaniami w obszarach zarządzania migracjami, zintegrowanego zarządzania granicami zewnętrznymi UE oraz zwalczania terroryzmu i przestępczości transgranicznej. Zdecydowana odpowiedź na wyżej wymienione wyzwania oraz budowanie rzeczywistej i skutecznej unii bezpieczeństwa wymagają skutecznej wymiany informacji między państwami członkowskimi, a także między państwami członkowskimi a odpowiednimi agencjami UE.

System Informacyjny Schengen (SIS) to najskuteczniejsze narzędzie zapewniające efektywną współpracę między organami imigracyjnymi, policją, organami celnymi i organami sądowymi w UE i państwach stowarzyszonych w ramach Schengen. Właściwe organy w państwach członkowskich, takie jak policja, straż graniczna i funkcjonariusze celni, powinny mieć dostęp do wysokiej jakości informacji na temat sprawdzanych przez siebie osób lub przedmiotów, a także do wyraźnych instrukcji dotyczących działań, które należy podjąć w każdym przypadku. Ten wielkoskalowy system informacyjny jest najważniejszym elementem współpracy Schengen i ma kluczowe znaczenie dla ułatwienia swobodnego przepływu osób w strefie Schengen. Umożliwia on właściwym organom wprowadzanie i przeglądanie danych dotyczących osób poszukiwanych, osób, które mogą nie mieć prawa do wjazdu lub pobytu na terytorium UE, osób zaginionych – w szczególności dzieci – oraz przedmiotów, które mogły zostać skradzione, sprzeniewierzone lub zgubione. Oprócz informacji na temat konkretnej osoby lub konkretnego przedmiotu SIS zawiera także wyraźne instrukcje określające sposób postępowania właściwych organów po odnalezieniu danej osoby lub danego przedmiotu.

Komisja przeprowadziła kompleksową ocenę[1] SIS w 2016 r., czyli trzy lata po uruchomieniu drugiej generacji systemu. W wyniku oceny wykazano, że pod względem operacyjnym SIS okazał się prawdziwym sukcesem. W 2015 r. właściwe organy krajowe sprawdzały dane osób i przedmiotów zgromadzone w SIS niemal 2,9 mld razy i dokonały wymiany ponad 1,8 mln informacji uzupełniających. Jak ogłoszono w programie prac Komisji na 2017 r., niezbędne jest jednak dalsze zwiększanie skuteczności i wydajności tego systemu w oparciu o te pozytywne doświadczenia. W tym celu Komisja przedstawia pierwszy zestaw składający się z trzech wniosków dotyczących poprawy i rozszerzenia stosowania SIS w wyniku oceny, kontynuując jednocześnie prowadzone prace nad zwiększeniem interoperacyjności istniejących i przyszłych systemów ścigania przestępstw i zarządzania granicami, polegające na prowadzeniu działań następczych w związku z bieżącymi pracami grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności.

Wnioski te dotyczą stosowania systemu na potrzeby: a) zarządzania granicami, b) współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych oraz c) powrotu nielegalnie przebywających obywateli państw trzecich. Dwa pierwsze wnioski łącznie tworzą

[1] Sprawozdanie 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 oraz towarzyszący mu dokument roboczy służb Komisji (Dz.U. …).

podstawę prawną utworzenia, funkcjonowania i użytkowania SIS. Wniosek dotyczący użytkowania SIS do celów powrotu nielegalnie przebywających obywateli państw trzecich uzupełnia wniosek dotyczący zarządzania granicami i stanowi dopełnienie zawartych w nim przepisów. Wniosek zawiera nową kategorię wpisów i stanowi wkład w wykonanie i monitorowanie dyrektywy 2008/115/WE[2].

W związku ze zmienną geometrią uczestnictwa państw członkowskich w polityce UE w obszarze wolności, bezpieczeństwa i sprawiedliwości należy przyjąć trzy odrębne instrumenty prawne, które będą jednak sprawnie się uzupełniać w celu umożliwienia kompleksowego funkcjonowania i użytkowania systemu.

Równolegle w celu usprawnienia i poprawy zarządzania informacjami na szczeblu UE w kwietniu 2016 r. Komisja zainicjowała proces refleksji „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa”[3]. Nadrzędnym celem jest zapewnienie, aby właściwe organy dysponowały stałym dostępem do niezbędnych informacji pochodzących z różnych systemów informacyjnych. Aby urzeczywistnić ten cel, Komisja prowadzi przeglądy istniejącej struktury informacyjnej w celu identyfikacji luk informacyjnych i słabych punktów wynikających z braków w funkcjach istniejących systemów oraz z fragmentacji ogólnej struktury zarządzania danymi w UE. Do celów wsparcia tych prac Komisja utworzyła grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności, której wstępne ustalenia dotyczące kwestii związanych z jakością danych wykorzystano przy sporządzaniu przedmiotowego pierwszego zestawu wniosków[4]. W swoim orędziu o stanie Unii z września 2016 r. przewodniczący Komisji Jean-Claude Juncker mówił między innymi o tym, jak ważne jest wyeliminowanie istniejących obecnie braków w zarządzaniu informacjami oraz poprawa interoperacyjności i wzajemnego połączenia istniejących systemów informacyjnych.

W odpowiedzi na ustalenia grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności, które zostaną przedstawione w pierwszej połowie 2017 r., w połowie 2017 r. Komisja rozważy przedstawienie drugiego zestawu wniosków w celu dalszej poprawy interoperacyjności między SIS a pozostałymi systemami informatycznymi. Równie istotnym elementem prowadzonych prac jest przegląd rozporządzenia (UE) nr 1077/2011[5] dotyczącego Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), który może stać się przedmiotem oddzielnych wniosków Komisji również w 2017 r. Ważnym elementem eliminacji aktualnych zagrożeń bezpieczeństwa jest inwestowanie w wysokiej jakości, sprawny i skuteczny proces wymiany informacji i zarządzania nimi oraz zapewnienie interoperacyjności baz danych i systemów informacyjnych UE.

---

2 Dyrektywa Parlamentu Europejskiego i Rady 2008/115/WE z dnia 16 grudnia 2008 r. w sprawie wspólnych norm i procedur stosowanych przez państwa członkowskie w odniesieniu do powrotów nielegalnie przebywających obywateli państw trzecich (Dz.U. L 348 z 24.12.2008, s. 98).

3 COM(2016) 205 final z 6.4.2016.

4 Decyzja Komisji 2016/C 257/03 z 17.6.2016.

5 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.U. L 286 z 1.11.2011, s. 1).

Aktualne ramy prawne drugiej generacji SIS, dotyczące jego stosowania do celów odpraw granicznych obywateli państw trzecich, oparte są o wcześniejszy instrument pierwszego filaru – rozporządzenie (WE) nr 1987/2006[6]. Niniejszy wniosek zastępuje[7] aktualny instrument prawny w celu:

- wprowadzenia obowiązku, by państwa członkowskie dokonywały wpisu w SIS we wszystkich przypadkach wydania zakazu wjazdu dla nielegalnie przebywającego obywatela państwa trzeciego zgodnie z przepisami zgodnymi z dyrektywą 2008/115/WE;

- harmonizacji procedur krajowych dotyczących korzystania z SIS w odniesieniu do procedury konsultacji, aby uniknąć sytuacji, w której obywatel państwa trzeciego objęty zakazem wjazdu posiada ważny dokument pobytowy wydany przez państwo członkowskie;

- wprowadzenia zmian technicznych, aby zwiększyć bezpieczeństwo i zmniejszyć obciążenia administracyjne;

- uwzględnienia pełnego użytkowania całego SIS, w tym nie tylko samego funkcjonowania systemu centralnego i systemu krajowego, lecz także potrzeb użytkowników końcowych poprzez zapewnienie, aby otrzymywali oni wszystkie dane, które są im niezbędne do wykonywania powierzonych im zadań, oraz aby przestrzegali oni wszystkich zasad bezpieczeństwa podczas przetwarzania danych SIS.

W niniejszym wniosku nie ustanawia się nowego systemu, tylko rozwija się i usprawnia system istniejący. Przegląd SIS wesprze i wzmocni działania Unii Europejskiej w ramach europejskich programów w zakresie migracji i bezpieczeństwa. Ponadto w ramach przeglądu:

1) przeprowadza się konsolidację wyników prac w zakresie wdrożenia SIS przeprowadzonych na przestrzeni ostatnich trzech lat i obejmujących wprowadzenie zmian technicznych do centralnego SIS w celu rozszerzenia niektórych już istniejących kategorii wpisów oraz utworzenia nowych funkcji;

2) wdraża się zalecenia dotyczące wprowadzenia technicznych i proceduralnych zmian w następstwie kompleksowej oceny SIS[8];

3) wdraża się usprawnienia techniczne, o które wnioskowali użytkownicy końcowi SIS; oraz

---

6 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.U. L 381 z 28.12.2006, s. 4).

7 W sekcji 2 „Wybór instrumentu" wyjaśniono, dlaczego zdecydowano się na zastąpienie zamiast przekształcenia obecnego prawodawstwa.

8 Sprawozdanie 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 oraz towarzyszący mu dokument roboczy służb Komisji (Dz.U. …).

4) wprowadza się wstępne ustalenia dotyczące jakości danych sformułowane przez grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności[9].

Ponieważ przedmiotowy wniosek jest nierozerwalnie powiązany z wnioskiem Komisji dotyczącym rozporządzenia w sprawie utworzenia, funkcjonowania i użytkowania SIS w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, wnioski zawierają szereg wspólnych przepisów. Przepisy te obejmują: środki dotyczące użytkowania całego SIS, w tym nie tylko samego funkcjonowania systemu centralnego i systemów krajowych, lecz także potrzeb użytkowników końcowych; wzmocnione środki na rzecz ciągłości działania; środki dotyczące jakości, ochrony i bezpieczeństwa danych oraz przepisy dotyczące monitorowania, oceny i sprawozdawczości. W obu wnioskach rozszerza się również wykorzystanie informacji biometrycznych[10].

Ze względu na eskalację kryzysu migracyjnego i uchodźczego w 2015 r. wyraźnie wzrosła konieczność podjęcia skutecznych kroków w celu rozwiązania problemu nielegalnej migracji. W Planie działania UE w zakresie powrotów[11] Komisja ogłosiła, że zaproponuje, by państwa członkowskie obowiązkowo wprowadzały do SIS wszystkie zakazy wjazdu, aby zapobiegać ponownemu wjazdowi do strefy Schengen obywateli państw trzecich, którzy nie mają prawa wjazdu i pobytu na terytorium państw członkowskich. Zakazy wjazdu wydane zgodnie z przepisami zgodnymi z dyrektywą 2008/115/WE obowiązują w całej strefie Schengen; w związku z tym mogą być egzekwowane na granicach zewnętrznych również przez organy państwa członkowskiego innego niż to, które wydało zakaz. Istniejące rozporządzenie (WE) nr 1987/2006 jedynie zezwala państwom członkowskim na dokonywanie w SIS wpisów dotyczących odmowy wjazdu i pobytu na podstawie zakazów wjazdu – ale tego nie wymaga. Dzięki wprowadzeniu obowiązku wpisywania wszystkich zakazów wjazdu do SIS można osiągnąć wyższy stopień skuteczności i harmonizacji.

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki oraz z obowiązującymi i przyszłymi instrumentami prawnymi**

Niniejszy wniosek jest w pełni spójny i zgodny z przepisami dyrektywy 2008/115/WE dotyczącymi wydawania i egzekwowania zakazów wjazdu. Uzupełnia więc istniejące przepisy w sprawie zakazów wjazdu i przyczynia się do skutecznego egzekwowania tych zakazów na granicach zewnętrznych, ułatwiając wykonywanie obowiązków określonych w dyrektywie powrotowej i skutecznie uniemożliwiając ponowny wjazd określonych obywateli państw trzecich do strefy Schengen.

- **Spójność z innymi politykami Unii**

Niniejszy wniosek jest ściśle powiązany z innymi obszarami polityki Unii oraz stanowi uzupełnienie innych obszarów polityki Unii, takich jak:

1) **bezpieczeństwo wewnętrzne** w odniesieniu do roli SIS w uniemożliwianiu wjazdu obywateli państw trzecich stwarzających zagrożenie bezpieczeństwa;

---

[9] Grupa ekspertów wysokiego szczebla – sprawozdanie przewodniczącego z dnia 21 grudnia 2016 r.

[10] Zob. sekcja 5 „Inne elementy”, w której przedstawiono szczegółowe wyjaśnienie dotyczące zmian uwzględnionych w niniejszym wniosku.

[11] COM(2015) 453 final.

2) **ochrona danych** w zakresie, w jakim w niniejszym wniosku zapewnia się ochronę praw podstawowych osób, których dane osobowe są przetwarzane w SIS.

3) Niniejszy wniosek jest również ściśle powiązany z obowiązującymi przepisami Unii oraz stanowi uzupełnienie obowiązujących przepisów Unii, takich jak:

4) **zarządzanie granicami zewnętrznymi** w zakresie, w jakim niniejszy wniosek wspiera państwa członkowskie w kontroli ich odcinków granic zewnętrznych UE oraz w zwiększaniu skuteczności unijnego systemu kontroli granic zewnętrznych;

5) skuteczna **polityka powrotowa UE** przyczyniająca się do wzmacniania systemu UE w zakresie wykrywania przypadków ponownego wjazdu obywateli państw trzecich po powrocie i zapobiegania takim przypadkom. Wniosek przyczyni się do ograniczenia zachęt dla nielegalnej migracji do UE, co jest jednym z głównych celów Europejskiego programu w zakresie migracji[12];

6) przepisy dotyczące **Europejskiej Straży Granicznej i Przybrzeżnej** w zakresie (i) możliwości przeprowadzania przez pracowników Agencji analiz ryzyka oraz (ii) dostępu jednostki centralnej ETIAS w ramach Agencji do SIS do celów proponowanego europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS)[13], a także (iii) w celu zapewnienia interfejsu technicznego umożliwiającego dostęp do SIS zespołom Europejskiej Straży Granicznej i Przybrzeżnej, zespołom składającym się z personelu realizującego zadania w dziedzinie powrotów oraz członkom zespołów wspierających zarządzanie migracjami, aby zespoły i osoby te miały prawo, w granicach powierzonych im uprawnień, do uzyskania dostępu do danych wprowadzanych do SIS oraz do wyszukiwania tego rodzaju danych;

7) przepisy dotyczące **Europolu** – zaproponowano, by miał on – w ramach przysługujących mu uprawnień – szersze prawa dostępu i wyszukiwania danych SIS.

Niniejszy wniosek jest ściśle powiązany z przyszłymi przepisami Unii oraz stanowi uzupełnienie przyszłych przepisów Unii, takich jak:

8) **system wjazdu/wyjazdu**, w ramach którego zaproponowano wykorzystanie połączenia odcisków palców i wizerunku twarzy jako identyfikatorów biometrycznych na potrzeby funkcjonowania systemu wjazdu/wyjazdu; w niniejszym wniosku starano się odzwierciedlić to podejście;

9) **ETIAS**, w ramach którego zaproponowano dokładną ocenę bezpieczeństwa, w tym weryfikację w SIS, przeprowadzaną w przypadku obywateli państw trzecich zwolnionych z obowiązku wizowego, którzy zamierzają podróżować na terytorium UE.

[12] COM(2015) 240 final.
[13] COM(2016) 731 final.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawę prawną dla przepisów dotyczących zintegrowanego zarządzania granicami i nielegalnej imigracji stanowią art. 77 ust. 2 lit. b) i d) oraz art. 79 ust. 2 lit. c) Traktatu o funkcjonowaniu Unii Europejskiej.

• Zmienna geometria

Niniejszy wniosek opiera się na przepisach dorobku Schengen związanych z odprawą graniczną. Z tego względu należy rozważyć następujące skutki wniosku w odniesieniu do różnych protokołów i umów z państwami stowarzyszonymi.

Dania: Zgodnie z art. 4 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatów, Dania podejmie decyzję, w terminie sześciu miesięcy po przyjęciu przez Radę decyzji w sprawie niniejszego rozporządzenia, czy dokona transpozycji niniejszego wniosku, stanowiącego rozwinięcie dorobku Schengen, do swojego prawa krajowego.

Zjednoczone Królestwo i Irlandia: Zgodnie z art. 4 i 5 Protokołu w sprawie dorobku Schengen włączonego w ramy Unii Europejskiej, decyzją Rady 2000/365/WE z dnia 29 maja 2000 r. dotyczącą wniosku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej oraz decyzją Rady 2002/192/WE z dnia 28 lutego 2002 r. dotyczącą wniosku Irlandii o zastosowanie wobec niej niektórych przepisów dorobku Schengen, rozporządzenia (UE) 2016/399 (kodeks graniczny Schengen) ani żadnych innych instrumentów prawnych potocznie określanych jako „dorobek Schengen", tj. instrumentów prawnych regulujących i wspierających działania na rzecz zniesienia kontroli na granicach wewnętrznych oraz środków wspierających związanych z kontrolami na granicach zewnętrznych, nie stosuje się wobec Zjednoczonego Królestwa i Irlandii. Niniejsze rozporządzenie stanowi rozwinięcie tego dorobku, Zjednoczone Królestwo i Irlandia nie uczestniczą zatem w przyjęciu niniejszego rozporządzenia, nie są nim związane ani go nie stosują.

Bułgaria i Rumunia: Niniejsze rozporządzenie stanowi akt oparty na dorobku Schengen lub w inny sposób z nim związany w rozumieniu art. 4 ust. 2 Aktu przystąpienia z 2005 r. Niniejsze rozporządzenie odczytuje się w związku z decyzją Rady 2010/365/UE z dnia 29 czerwca 2010 r.[14], która zawiera wykaz przepisów dorobku Schengen związanych z Systemem Informacyjnym Schengen, które mają mieć zastosowanie w Bułgarii i Rumunii, z zastrzeżeniem określonych ograniczeń.

Cypr i Chorwacja: Niniejsze rozporządzenie stanowi akt oparty na dorobku Schengen lub w inny sposób z nim związany w rozumieniu odpowiednio art. 3 ust. 2 Aktu przystąpienia z 2003 r. oraz art. 4 ust. 2 Aktu przystąpienia z 2011 r.

Państwa stowarzyszone: Na podstawie odpowiednich umów dotyczących włączenia tych państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen Islandia, Norwegia i Liechtenstein mają być związane proponowanym rozporządzeniem.

---

[14] Decyzja Rady z dnia 29 czerwca 2010 r. w sprawie stosowania w Republice Bułgarii i w Rumunii przepisów dorobku Schengen związanych z systemem informacyjnym Schengen (Dz.U. L 166 z 1.7.2010, s. 17).

- **Pomocniczość**

W ramach niniejszego wniosku rozwija się istniejący SIS i bazuje się na tym systemie, uruchomionym w 1995 r. W dniu 9 kwietnia 2013 r. pierwotne ramy międzyrządowe zastąpiono instrumentami unijnymi (rozporządzeniem (WE) nr 1987/2006 i decyzją Rady 2007/533/WSiSW). Przy wcześniejszych okazjach przeprowadzono pełną analizę zgodności z zasadą pomocniczości. Celem przedmiotowej inicjatywy jest dalsze udoskonalenie obowiązujących przepisów poprzez wyeliminowanie zidentyfikowanych braków i poprawę procedur operacyjnych.

Osiągnięcie znacznego poziomu wymiany informacji między państwami członkowskimi nie jest możliwe za pomocą zdecentralizowanych rozwiązań. Ze względu na skalę, skutki i wpływ przedmiotowego działania cele niniejszego wniosku można lepiej osiągnąć na szczeblu unijnym.

Cele niniejszego wniosku obejmują między innymi usprawnienia techniczne w celu zwiększenia wydajności SIS oraz wysiłki służące harmonizacji użytkowania systemu we wszystkich uczestniczących państwach członkowskich. Z uwagi na transgraniczny charakter wymienionych celów i wyzwań związanych z zapewnieniem skutecznej wymiany informacji w celu zwalczania coraz bardziej różnorodnych zagrożeń UE jest właściwym podmiotem, by zaproponować rozwiązania kwestii opisanych powyżej, których państwa członkowskie, działając osobno, nie są w stanie rozwiązać w wystarczającym stopniu.

Jeżeli istniejące ograniczenia SIS nie zostaną wyeliminowane, istnieje ryzyko niewykorzystania wielu możliwości osiągnięcia maksymalnej wydajności i europejskiej wartości dodanej oraz utrudniania pracy właściwych organów przez istniejące braki. Przykładowo brak zharmonizowanych przepisów dotyczących usuwania starych wpisów w systemie może utrudniać swobodny przepływ osób stanowiący podstawową zasadę Unii.

- **Proporcjonalność**

Artykuł 5 Traktatu o Unii Europejskiej stanowi, że działanie Unii nie wykracza poza to, co jest konieczne do osiągnięcia celów Traktatu. Forma wybrana dla tego działania UE musi zatem umożliwić osiągnięcie celów wniosku i jego wprowadzenie w życie w jak najskuteczniejszy sposób. Proponowana inicjatywa stanowi zmianę SIS w odniesieniu do odpraw granicznych.

Niniejszy wniosek opiera się na zasadach *uwzględnienia ochrony prywatności już w fazie projektowania*. Niniejszy wniosek jest proporcjonalny pod względem prawa do ochrony danych osobowych, ponieważ zawiera przepisy szczegółowe dotyczące usuwania wpisów oraz nie wymaga gromadzenia i przechowywania danych przez okres dłuższy, niż jest to absolutnie konieczne do funkcjonowania systemu i osiągnięcia jego celów. Wpisy w SIS zawierają wyłącznie dane wymagane do identyfikacji i lokalizacji osoby lub przedmiotu oraz do podjęcia odpowiedniego działania operacyjnego. Wszystkie inne dodatkowe dane podają biura SIRENE, umożliwiając wymianę informacji uzupełniających.

Ponadto w niniejszym wniosku przewiduje się wdrożenie wszystkich zabezpieczeń i mechanizmów niezbędnych, by zapewnić skuteczną ochronę praw podstawowych osób, których dane dotyczą, a w szczególności przysługujące im prawo do ochrony życia prywatnego i danych osobowych. Niniejszy wniosek zawiera również przepisy służące konkretnie wzmocnieniu bezpieczeństwa przechowywanych w SIS danych osobowych osób fizycznych.

Zapewnienie funkcjonowania systemu nie będzie wymagało żadnych dodatkowych procedur ani harmonizacji na szczeblu UE. Proponowany środek należy uznać za proporcjonalny, ponieważ nie wykracza on poza to, co jest konieczne do zapewnienia, aby działanie podejmowane na szczeblu UE umożliwiło osiągnięcie wyznaczonych celów.

- **Wybór instrumentu**

Proponowana zmiana również będzie mieć formę rozporządzenia i zastąpi rozporządzenie (WE) nr 1987/2006. Podejście to przyjęto również w odniesieniu do decyzji Rady 2007/533/WSiSW; ponieważ oba te instrumenty są ze sobą ściśle związane, trzeba je przyjąć także w odniesieniu do rozporządzenia (WE) nr 1987/2006. Decyzję 2007/533/WSiSW przyjęto jako tak zwany „instrument trzeciego filaru" na podstawie poprzedniej wersji Traktatu o Unii Europejskiej. Tego rodzaju instrumenty „trzeciego filaru" Rada przyjmowała samodzielnie, bez Parlamentu Europejskiego w charakterze współprawodawcy. Podstawą prawną niniejszego wniosku jest Traktat o funkcjonowaniu Unii Europejskiej (TFUE), ponieważ struktura oparta na filarach przestała istnieć wraz z wejściem w życie Traktatu z Lizbony w dniu 1 grudnia 2009 r. W ramach podstawy prawnej wymaga się zastosowania zwykłej procedury ustawodawczej. Nadanie formy rozporządzenia (Parlamentu Europejskiego i Rady) jest koniecznie, ponieważ przepisy te mają być wiążące i bezpośrednio stosowane we wszystkich państwach członkowskich.

Niniejszy wniosek będzie opierał się na istniejącym scentralizowanym systemie i będzie wzmacniał ten system, w ramach którego państwa członkowskie będą ze sobą współpracowały, co wiąże się z koniecznością ustanowienia wspólnej struktury i wiążących zasad funkcjonowania. Ponadto we wniosku określono obowiązkowe zasady dotyczące dostępu do systemu, w tym na potrzeby ścigania przestępstw, jednakowe dla wszystkich państw członkowskich i Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości[15] (eu-LISA). Od dnia 9 maja 2013 r. eu-LISA odpowiada za zarządzanie operacyjne systemem centralnym SIS, co obejmuje wszystkie zadania niezbędne do zapewnienia pełnego funkcjonowania systemu centralnego SIS przez całą dobę siedem dni w tygodniu. Niniejszy wniosek opiera się na obowiązkach eu-LISA dotyczących SIS.

Ponadto wniosek zawiera bezpośrednio stosowane przepisy przewidujące możliwość uzyskania dostępu przez osoby, których dane dotyczą, do ich danych oraz do środków odwoławczych, które to przepisy nie wymagają przyjęcia dalszych środków wykonawczych w tym zakresie.

W konsekwencji jako instrument prawny można wybrać jedynie rozporządzenie.

[15] Ustanowionej rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. ustanawiającym Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz.U. L 286 z 1.11.2011, s. 1).

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

• Oceny *ex post* / kontrole sprawności obowiązującego prawodawstwa

Zgodnie z rozporządzeniem (WE) nr 1987/2006 i decyzją Rady 2007/533/WSiSW[16] trzy lata po rozpoczęciu eksploatacji centralnego systemu SIS II Komisja przeprowadziła ogólną ocenę tego systemu oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi.

Ocena obejmowała w szczególności przegląd stosowania art. 24 rozporządzenia (WE) nr 1987/2006 w celu przedstawienia koniecznych wniosków w sprawie zmiany przepisów niniejszego artykułu, tak aby osiągnąć wyższy poziom harmonizacji kryteriów dokonywania wpisów.

Wyniki oceny uwidoczniły konieczność wprowadzenia zmian do podstawy prawnej SIS w celu zapewnienia lepszego reagowania na nowe wyzwania w zakresie bezpieczeństwa i migracji. Obejmuje to na przykład propozycje dotyczące wprowadzenia obowiązku wpisywania zakazów wjazdu do SIS, aby skuteczniej je egzekwować, obowiązkowych konsultacji między państwami członkowskimi, aby uniknąć sytuacji, w której posiadacz dokumentu pobytowego jest jednocześnie objęty zakazem wjazdu, opcji identyfikowania i lokalizowania osób fizycznych na podstawie ich odcisków palców za pomocą nowego systemu automatycznej identyfikacji daktyloskopijnej oraz poszerzenia zakresu identyfikatorów biometrycznych w systemie.

W wyniku wspomnianej oceny wykazano również potrzebę zmian prawnych mających na celu poprawę technicznego funkcjonowania systemu oraz usprawnienia procesów krajowych. Środki te zwiększą wydajność i skuteczność SIS dzięki ułatwieniu jego użytkowania i ograniczeniu zbędnych obciążeń. Kolejne środki mają poprawić jakość danych i przejrzystość systemu dzięki doprecyzowaniu opisów konkretnych zadań w zakresie sprawozdawczości należących do państw członkowskich i eu-LISA.

Wyniki kompleksowej oceny (sprawozdanie z oceny i powiązany dokument roboczy służb Komisji przyjęto w dniu 21 grudnia 2016 r.[17]) stanowią podstawę środków zawartych w niniejszym wniosku.

Ponadto zgodnie z art. 19 dyrektywy powrotowej 2008/115/WE Komisja opublikowała w 2014 r. komunikat w sprawie polityki UE w zakresie powrotów[18], w którym przedstawiono stosowanie tej dyrektywy. W komunikacie tym stwierdzono, że potencjał SIS w dziedzinie polityki powrotowej powinien zostać zwiększony oraz że przegląd SIS II jest okazją do zwiększenia spójności polityki powrotowej i SIS II. Zasugerowano też nałożenie na państwa członkowskie obowiązku dokonywania w SIS II wpisów dotyczących odmowy wjazdu w odniesieniu do zakazów wjazdu wydanych na podstawie dyrektywy powrotowej.

---

16 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. L 205 z 7.8.2007, s. 63).

17 Sprawozdanie 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 oraz towarzyszący mu dokument roboczy służb Komisji.

18 COM(2014) 199 final.

- **Konsultacje z zainteresowanymi stronami**

W toku oceny SIS prowadzonej przez Komisję zwrócono się do odpowiednich zainteresowanych stron, w tym do delegatów do Komitetu SIS–VIS, w ramach procedury ustanowionej w art. 51 rozporządzenia (WE) nr 1987/2006, o przedstawienie informacji zwrotnych i sugestii. Komitet ten składa się z przedstawicieli państw członkowskich zajmujących się zarówno operacyjnymi kwestiami dotyczącymi SIRENE (współpraca transgraniczna w odniesieniu do SIS) oraz kwestiami technicznymi z zakresu opracowania i utrzymania SIS, jak również powiązanego z nim zastosowania SIRENE.

W ramach procesu oceny delegaci udzielili odpowiedzi na szczegółowe pytania zawarte w kwestionariuszach. Konieczne dalsze wyjaśnienia lub rozwinięcie tematu odbywało się w drodze wymiany korespondencji elektronicznej lub ukierunkowanych wywiadów.

Ten złożony i wieloetapowy proces umożliwił podnoszenie kwestii w kompleksowy i przejrzysty sposób. Na przestrzeni lat 2015 i 2016 delegaci do Komitetu SIS–VIS omawiali tego rodzaju kwestie na specjalnych posiedzeniach i warsztatach.

Komisja prowadziła również szczególne konsultacje z krajowymi organami ochrony danych państw członkowskich i członkami Grupy ds. Koordynowania Nadzoru SIS II w dziedzinie ochrony danych. Udzielając odpowiedzi na specjalny kwestionariusz, państwa członkowskie wymieniły się swoimi doświadczeniami w zakresie wniosków o uzyskanie dostępu oraz prac krajowych organów ochrony danych. Informacje zawarte w odpowiedziach na przedmiotowy kwestionariusz udzielone od czerwca 2015 r. wykorzystano przy opracowywaniu niniejszego wniosku.

W ramach swoich struktur wewnętrznych Komisja ustanowiła międzyresortową grupę sterującą składającą się z przedstawicieli Sekretariatu Generalnego, Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych, Dyrekcji Generalnej ds. Sprawiedliwości i Konsumentów, Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa oraz Dyrekcji Generalnej ds. Informatyki. Grupa sterująca monitorowała proces oceny i w razie potrzeby udzielała wytycznych.

W ustaleniach z oceny wzięto również pod uwagę dowody zgromadzone w trakcie wizyt na miejscu prowadzonych w ramach oceny w państwach członkowskich w celu szczegółowego zbadania praktycznego wykorzystania SIS. Dowody te pochodziły między innymi z dyskusji i wywiadów z praktykami, personelem biura SIRENE i właściwych organów krajowych.

Informacje zwrotne i sugestie odpowiednich organów państw członkowskich właściwych ds. powrotów, w szczególności te na temat konsekwencji ewentualnego obowiązku dokonywania w SIS wpisów dotyczących zakazów wjazdu wydanych zgodnie z dyrektywą 2008/115/WE, uzyskano także w ramach Grupy Kontaktowej Komisji ds. Dyrektywy Powrotowej na jej posiedzeniach w dniach 16 listopada 2015 r. oraz 18 marca i 20 czerwca 2016 r.

W związku z otrzymanymi informacjami zwrotnymi w niniejszym wniosku przewiduje się środki na rzecz poprawy technicznej i operacyjnej wydajności i skuteczności systemu.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Oprócz prowadzenia konsultacji z zainteresowanymi stronami Komisja dążyła również do uzyskania wiedzy eksperckiej w ramach czterech badań, których ustalenia uwzględniono przy opracowywaniu niniejszego wniosku:

- Ocena techniczna SIS (Kurt Salmon)[19]

W ramach przedmiotowej oceny określono kluczowe kwestie związane z funkcjonowaniem SIS oraz przyszłe potrzeby, które należy zaspokoić, a w szczególności problemy związane z maksymalizacją ciągłości działania i zapewnieniem możliwości dostosowania całej architektury do coraz większych wymogów dotyczących zdolności.

- Ocena wpływu technologii informacyjno-komunikacyjnych na potencjalne usprawnienia w architekturze SIS II (Kurt Salmon)[20]

W przedmiotowym badaniu ocenie poddano bieżący koszt funkcjonowania SIS na szczeblu krajowym oraz przeanalizowano dwa możliwe scenariusze techniczne mające na celu udoskonalenie tego systemu. W obu scenariuszach zakłada się przedstawienie zestawu technicznych wniosków koncentrujących się na poprawie systemu centralnego i ogólnej architektury.

- Ocena wpływu technologii informacyjno-komunikacyjnych na potencjalne usprawnienia w architekturze SIS II – sprawozdanie końcowe, 10 listopada 2016 r., (Wavestone)[21]

W przedmiotowym badaniu przeprowadzono ocenę kosztu, który wiąże się dla państw członkowskich z wdrożeniem kopii krajowej, poprzez przeanalizowanie trzech scenariuszy (w pełni scentralizowanego systemu, wdrożenia standardowego N.SIS opracowanego i zapewnionego na potrzeby państw członkowskich przez eu-LISA oraz wdrożenia odrębnych N.SIS w oparciu o wspólne standardy techniczne).

- Badanie dotyczące wykonalności i skutków ustanowienia w ramach Systemu Informacyjnego Schengen ogólnounijnego systemu wymiany danych dotyczących monitorowania przestrzegania decyzji nakazujących powrót (PwC)[22]

W badaniu tym oceniono wykonalność oraz techniczne i operacyjne skutki proponowanych zmian w SIS mających na celu usprawnienie jego użytkowania w odniesieniu do powrotów nielegalnych migrantów i zapobiegania ponownemu wjazdowi tych migrantów.

- **Ocena skutków**

Komisja nie przeprowadziła oceny skutków.

Trzy wyżej wymienione niezależne oceny stanowią podstawę rozważań na temat skutków zmian w systemie z technicznego punktu widzenia. Ponadto Komisja przeprowadziła dwa

[19] SPRAWOZDANIE KOŃCOWE Komisji Europejskiej – Ocena techniczna SIS II.

[20] SPRAWOZDANIE KOŃCOWE Komisji Europejskiej – Ocena wpływu technologii informacyjno-komunikacyjnych na potencjalne usprawnienia w architekturze SIS II z 2016 r.

[21] SPRAWOZDANIE KOŃCOWE Komisji Europejskiej – Ocena wpływu technologii informacyjno-komunikacyjnych na potencjalne usprawnienia w architekturze SIS II – sprawozdanie końcowe, 10 listopada 2016 r., (Wavestone)

[22] Badanie dotyczące wykonalności i skutków ustanowienia w ramach SIS ogólnounijnego systemu wymiany danych dotyczących monitorowania przestrzegania decyzji nakazujących powrót, 4 kwietnia 2015 r., PwC.

przeglądy podręcznika SIRENE od roku 2013, tj. od momentu uruchomienia SIS II w dniu 9 kwietnia 2013 r. i od kiedy zaczęto stosować decyzję 2007/533/WSiSW. Jednym z powyższych przeglądów był przegląd śródokresowy, w wyniku którego w dniu 29 stycznia 2015 r. wprowadzono nowy podręcznik SIRENE[23]. Komisja przyjęła również Katalog zaleceń i najlepszych praktyk[24]. Ponadto eu-LISA i państwa członkowskie wprowadzają regularne, złożone usprawnienia techniczne systemu. Uznaje się, że warianty te nie zostały w pełni wykorzystane i należy przeprowadzić bardziej całościową zmianę podstawy prawnej. Osiągnięcie przejrzystości w obszarach takich jak zastosowanie systemów dla użytkowników końcowych i przepisy szczegółowe dotyczące usuwania wpisów nie jest możliwe wyłącznie za sprawą poprawy wdrażania i egzekwowania przepisów.

Ponadto Komisja przeprowadziła kompleksową ocenę SIS 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 oraz opublikowała towarzyszący dokument roboczy służb Komisji. Wyniki kompleksowej oceny (sprawozdanie z oceny i powiązany dokument roboczy służb Komisji przyjęte w dniu 21 grudnia 2016 r.) stanowią podstawę środków zawartych w niniejszym wniosku.

Mechanizm oceny Schengen, ustanowiony rozporządzeniem (UE) nr 1053/2013[25], umożliwia przeprowadzenie okresowej prawnej i operacyjnej oceny funkcjonowania SIS w państwach członkowskich. Tego rodzaju oceny przeprowadzane są wspólnie przez Komisję i państwa członkowskie. Za pośrednictwem powyższego mechanizmu Rada wydaje zalecenia adresowane do poszczególnych państw członkowskich na podstawie ocen przeprowadzonych w ramach wieloletnich i rocznych programów. Biorąc pod uwagę indywidualny charakter tego rodzaju zaleceń, nie mogą one zastąpić prawnie wiążących przepisów, które mają zastosowanie równocześnie do wszystkich państw członkowskich używających SIS.

Komitet SIS–VIS regularnie omawia praktyczne kwestie operacyjne i techniczne. Chociaż tego rodzaju posiedzenia mają istotne znaczenie we współpracy między Komisją a państwami członkowskimi, w wyniku prowadzonych dyskusji (w których nie podejmuje się kwestii zmian legislacyjnych) nie jest możliwe rozwiązanie kwestii pojawiających się na przykład w związku z różnymi praktykami krajowymi.

Zmiany proponowane w niniejszym rozporządzeniu nie wiążą się z istotnymi skutkami gospodarczymi ani oddziaływaniem na środowisko. Oczekuje się jednak, że proponowane zmiany będą miały istotne pozytywne skutki społeczne, ponieważ ich wprowadzenie zapewni większe bezpieczeństwo za sprawą lepszej identyfikacji osób posługujących się fałszywą tożsamością, przestępców, których tożsamość pozostaje nieznana po dokonaniu przez nich poważnego przestępstwa, oraz nielegalnych migrantów wykorzystujących istnienie obszaru

---

[23] 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.U. L 44 z 18.2.2015, s. 75).

[24] Zalecenie Komisji w sprawie ustanowienia Katalogu zaleceń i najlepszych praktyk dotyczących właściwego stosowania systemu informacyjnego Schengen (SIS II) oraz wymiany informacji uzupełniających przez właściwe organy państw członkowskich wdrażające i wykorzystujące SIS II [C(2015)9169/1].

[25] Rozporządzenie (UE) nr 1053/2013 z dnia 7 października 2013 r. w sprawie ustanowienia mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen oraz uchylenia decyzji komitetu wykonawczego z dnia 16 września 1998 r. dotyczącej utworzenia Stałego Komitetu ds. Oceny i Wprowadzania w Życie Dorobku Schengen (Dz.U. L 295 z 6.11.2013, s. 27).

bez kontroli na granicach wewnętrznych. Wpływ tych zmian na prawa podstawowe i ochronę danych został rozważony i przedstawiony bardziej szczegółowo w następnej sekcji („Prawa podstawowe").

Przy sporządzaniu niniejszego wniosku wykorzystano znaczną część dowodów zgromadzonych na potrzeby ogólnej oceny SIS drugiej generacji, w ramach której zbadano funkcjonowanie systemu i ewentualne obszary wymagające usprawnienia. Ponadto przeprowadzono ocenę skutków pod względem kosztów, aby zagwarantować wybór najbardziej odpowiedniej i proporcjonalnej architektury krajowej.

- **Prawa podstawowe i ochrona danych**

W niniejszym wniosku nie ustanawia się nowego systemu, tylko rozwija się i usprawnia system istniejący, bazując tym samym na już wprowadzonych istotnych i skutecznych zabezpieczeniach. Ponieważ jednak system ten nadal służy do przetwarzania danych osobowych i będą w nim przetwarzane kolejne kategorie wrażliwych danych biometrycznych, trzeba liczyć się z ewentualnym wpływem na prawa podstawowe osób fizycznych. Tego rodzaju wpływ został dokładnie przeanalizowany, a ponadto wprowadzono dodatkowe zabezpieczenia, aby gromadzenie i dalsze przetwarzanie danych było ograniczone do tego, co jest absolutnie koniecznie i niezbędne z operacyjnego punktu widzenia, oraz ograniczono dostęp do tego rodzaju danych do osób, które muszą przetwarzać takie dane ze względów operacyjnych. W niniejszym wniosku określono wyraźne ramy czasowe przechowywania danych oraz wyraźnie uznaje się i zapewnia prawa osób fizycznych do uzyskania dostępu do danych, które ich dotyczą, i poprawiania takich danych, a także do żądania ich usunięcia zgodnie z przysługującymi takim osobom prawami podstawowymi (zob. sekcja dotycząca ochrony i bezpieczeństwa danych).

Ponadto we wniosku wzmacnia się środki na rzecz ochrony praw podstawowych poprzez określenie w przepisach wymogów dotyczących usunięcia wpisu oraz wprowadzenie oceny proporcjonalności w przypadku rozszerzenia wpisu. W niniejszym wniosku określa się szerokie i solidne zabezpieczenia dotyczące wykorzystania identyfikatorów biometrycznych, aby nie przysparzać niedogodności niewinnym osobom.

We wniosku wymaga się ponadto bezpieczeństwa całego systemu, zapewniając większy poziom ochrony danych przechowywanych w systemie. W związku z wprowadzeniem przejrzystej procedury zarządzania zdarzeniami oraz poprawą ciągłości działania SIS niniejszy wniosek jest w pełni zgodny z Kartą praw podstawowych Unii Europejskiej[26] nie tylko w odniesieniu do prawa do ochrony danych osobowych. Rozwój i nieprzerwana skuteczność SIS zwiększą bezpieczeństwo osób fizycznych w społeczeństwie.

W niniejszym wniosku przewidziano istotne zmiany dotyczące identyfikatorów biometrycznych. Oprócz odcisków palców należy również gromadzić i przechowywać odciski dłoni, z zastrzeżeniem spełnienia wymogów prawnych. Rejestry odcisków palców są dołączane do alfanumerycznych wpisów w SIS zgodnie z art. 24. W przyszłości należy umożliwić wyszukiwanie tego rodzaju danych daktyloskopijnych (odcisków palców i dłoni) w celu dopasowania śladów linii papilarnych znalezionych na miejscu przestępstwa, pod warunkiem że popełnione przestępstwo wyczerpuje znamiona poważnego przestępstwa lub przestępstwa terrorystycznego, oraz jeżeli z dużym prawdopodobieństwem można stwierdzić, że znalezione ślady linii papilarnych należą do sprawcy. Jeżeli na podstawie dokumentów

[26] Karta praw podstawowych Unii Europejskiej (2012/C 326/02).

danej osoby nie można z całą pewnością ustalić jej tożsamości, właściwe organy powinny sprawdzić, czy jej odciski placów można dopasować do odcisków palców przechowywanych w bazie danych SIS.

Zgodnie z niniejszym wnioskiem wymaga się gromadzenia i przechowywania danych dodatkowych (takich jak informacje zawarte w dokumentach tożsamości), które ułatwiają ustalenie tożsamości danej osoby przez funkcjonariuszy pracujących w terenie.

W niniejszym wniosku gwarantuje się osobom, których dane dotyczą, prawo do skutecznego środka odwoławczego dostępnego w celu zaskarżenia wszelkich decyzji, przy czym do tego rodzaju środków prawnych zawsze powinien należeć skuteczny środek prawny na drodze sądowej zgodnie z art. 47 Karty praw podstawowych.

4. WPŁYW NA BUDŻET

SIS stanowi jednolity system informacyjny. W związku z powyższym wydatki przewidziane w dwóch wnioskach (w niniejszym wniosku i we wniosku dotyczącym rozporządzenia w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych) należy uznać za jedną kwotę, a nie dwie oddzielne. Wpływ na budżet związany ze zmianami, których wymaga wdrożenie obydwu wniosków, ujęto w jednej ocenie skutków finansowych regulacji.

Ze względu na uzupełniający charakter trzeciego wniosku (dotyczącego powrotu nielegalnie przebywających obywateli państw trzecich) związany z nim wpływ na budżet rozpatrzono oddzielnie w niezależnej ocenie skutków finansowych dotyczącej wyłącznie ustanowienia przedmiotowej specjalnej kategorii wpisów.

Na podstawie oceny różnych aspektów prac wymaganych w związku z siecią, centralnym SIS zarządzanym przez eu-LISA i zmianami krajowymi w państwach członkowskich ustalono, że dwa przedmiotowe wnioski dotyczące rozporządzeń będą wymagały przeznaczenia łącznej kwoty 64,3 mln EUR w latach 2018–2020.

W kwocie tej uwzględniono koszt zwiększenia przepustowości TESTA-NG wymaganego w związku z faktem, że zgodnie z przedmiotowymi dwoma wnioskami przesyłane w sieci pliki z odciskami palców i wizerunkami twarzy będą wymagały wyższej przepustowości i wydajności (9,9 mln EUR). W kwocie tej uwzględniono również koszty ponoszone przez eu-LISA, obejmujące koszty personelu i wydatki operacyjne (17,6 mln EUR); eu-LISA poinformowała Komisję, że na styczeń 2018 r. zaplanowano rekrutację 3 nowych pracowników kontraktowych w celu terminowego rozpoczęcia fazy opracowywania, aby zapewnić uruchomienie zaktualizowanych funkcji SIS w 2020 r. Z niniejszym wnioskiem wiąże się wprowadzenie zmian technicznych do centralnego SIS w celu rozszerzenia niektórych już istniejących kategorii wpisów oraz utworzenia nowych funkcji. Zmiany te uwzględniono w ocenie skutków finansowych dołączonej do wniosku.

Ponadto Komisja przeprowadziła ocenę skutków pod względem kosztów w celu oszacowania kosztów zmian na szczeblu krajowym, których wprowadzenia wymaga niniejszy wniosek[27]. Szacunkowy koszt wynosi 36,8 mln EUR, przy czym kwotę tę należy rozdzielić między państwa członkowskie w formie płatności ryczałtowej. Każde państwo członkowskie otrzyma zatem kwotę 1,2 mln EUR na modernizację swojego systemu krajowego zgodnie z wymogami określonymi w niniejszym wniosku, w tym z wymogiem utworzenia częściowej kopii krajowej, jeżeli taka kopia nie została jeszcze utworzona, lub systemu rezerwowego.

W celu przeprowadzenia modernizacji i wdrożenia funkcji przewidzianych w przedmiotowych dwóch wnioskach zaplanowano przeprogramowanie pozostałej części puli środków przeznaczonych w ramach Funduszu Bezpieczeństwa Wewnętrznego na inicjatywę na rzecz inteligentnych granic. Rozporządzenie w sprawie Funduszu Bezpieczeństwa Wewnętrznego i wsparcia w zakresie granic[28] jest instrumentem finansowym, w którym uwzględniono budżet przeznaczony na realizację pakietu dotyczącego inteligentnych granic. W art. 5 rozporządzenia przewidziano, że kwota 791 mln EUR zostanie wdrożona poprzez realizację programu tworzenia systemów informatycznych wspierających zarządzanie przepływami migracyjnymi przez granice zewnętrzne na warunkach określonych w art. 15. Z podanej powyżej kwoty 791 mln EUR kwota 480 mln EUR jest zarezerwowana na rozwój systemu wjazdu/wyjazdu, a kwota 210 mln EUR – na rozwój europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS). Część pozostałej kwoty zostanie przeznaczona na pokrycie kosztów zmian przewidzianych w przedmiotowych dwóch wnioskach dotyczących SIS.

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Komisja, państwa członkowskie i eu-LISA będą prowadzić regularne przeglądy i monitorowanie użytkowania SIS, aby zapewnić jego skuteczne i wydajne funkcjonowanie. Komitet SIS–VIS będzie wspierał Komisję we wdrażaniu środków technicznych i operacyjnych, jak przewidziano w niniejszym wniosku.

Ponadto niniejsze proponowane rozporządzenie zawiera w art. 54 ust. 7 i 8 przepisy dotyczące przeprowadzania formalnego, regularnego procesu przeglądu i oceny.

Co dwa lata eu-LISA ma obowiązek przedkładać Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące technicznej sprawności – w tym bezpieczeństwa – SIS, infrastruktury łączności systemu oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi.

Ponadto co cztery lata Komisja ma obowiązek przeprowadzić oraz przekazać Parlamentowi i Radzie ogólną ocenę SIS i wymiany informacji między państwami członkowskimi. Umożliwi to:

---

[27] Wavestone „Ocena wpływu technologii informacyjno-komunikacyjnych na potencjalne usprawnienia w architekturze SIS II – sprawozdanie końcowe”, 10 listopada 2016 r., Scenariusz 3 – Wdrożenie odrębnych N. SIS II.

[28] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 515/2014 z dnia 16 kwietnia 2014 r. ustanawiające, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument na rzecz wsparcia finansowego w zakresie granic zewnętrznych i wiz (Dz.U. L 150 z 20.5.2014, s. 143).

- analizę osiągniętych wyników w zestawieniu z celami;
- określenie, na ile wciąż aktualne są pierwotne przesłanki systemu;
- analizę sposobu, w jaki niniejsze rozporządzenie stosowane jest do systemu centralnego;
- ocenę bezpieczeństwa systemu centralnego;
- ocenę konsekwencji dla przyszłego funkcjonowania systemu.

Obecnie eu-LISA powierzono również obowiązek dostarczania dziennych, miesięcznych i rocznych statystyk na temat sposobu wykorzystania SIS, co zapewnia stałe monitorowanie systemu i jego funkcjonowania w zestawieniu z celami.

- **Szczegółowe objaśnienia nowych przepisów wniosku**

Przepisy wspólne dla niniejszego wniosku i wniosku dotyczącego rozporządzenia w sprawie utworzenia, funkcjonowania i użytkowania SIS w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych

- Przepisy ogólne (art. 1–3)
- Struktura techniczna i sposoby korzystania z SIS (art. 4–14)
- Obowiązki eu-LISA (art. 15–18)
- Prawo do dostępu do wpisów i przechowywanie wpisów (art. 29, 30, 31, 33 i 34)
- Ogólne zasady przetwarzania i ochrony danych (art. 36–53)
- Monitorowanie i statystyka (art. 54)

Pełne użytkowanie SIS

Posiadający ponad 2 mln użytkowników końcowych we właściwych organach w całej Europie SIS to niezwykle powszechnie stosowane i skuteczne narzędzie wymiany informacji. Przedmiotowe wnioski obejmują przepisy dotyczące pełnego funkcjonowania systemu, w tym centralnego SIS obsługiwanego przez eu-LISA, systemów krajowych i zastosowań dla użytkownika końcowego. System ten obejmuje nie tylko system centralny i systemy krajowe, ale także zaspokaja techniczne i operacyjne potrzeby użytkowników końcowych.

Artykuł 9 ust. 2 stanowi, że użytkownicy końcowi muszą otrzymywać dane potrzebne do wykonania ich zadań (w szczególności wszystkie dane potrzebne do identyfikacji osoby, której dane dotyczą, oraz do podjęcia odpowiednich działań). W artykule tym przewiduje się wdrażanie SIS przez państwa członkowskie w oparciu o wspólny plan działania zapewniający harmonizację wszystkich systemów krajowych. Artykuł 6 stanowi, że każde państwo członkowskie musi zapewnić użytkownikom końcowym nieprzerwany dostęp do danych SIS, co ma zmaksymalizować korzyści operacyjne poprzez ograniczenie możliwości przestoju.

Artykuł 10 ust. 3 zapewnia, by bezpieczeństwo przetwarzania danych dotyczyło również działań prowadzonych przez użytkownika końcowego w zakresie przetwarzania danych.

Artykuł 14 zobowiązuje państwa członkowskie do zapewnienia, aby personel mający dostęp do SIS odbywał regularne i ustawiczne szkolenia w zakresie zasad bezpieczeństwa i ochrony danych.

W związku z uwzględnieniem tych środków oraz wprowadzeniem zasad i obowiązków dotyczących milionów użytkowników końcowych w całej Europie w niniejszym wniosku bardziej kompleksowo traktuje się kwestię pełnego funkcjonowania SIS. Aby jak najskuteczniej wykorzystywać SIS, państwa członkowskie powinny zapewnić, aby za każdym razem, kiedy użytkownicy końcowi są uprawnieni do przeprowadzenia wyszukiwania w krajowej bazie danych policji lub bazie danych imigracyjnych, równolegle prowadzili wyszukiwanie w SIS. Dzięki temu SIS może działać zgodnie ze swoim przeznaczeniem jako główny środek uzupełniający na obszarze bez kontroli na granicach wewnętrznych, a państwa członkowskie mogą lepiej uwzględniać transgraniczny wymiar przestępczości i mobilności przestępców. Tego rodzaju wyszukiwanie równoległe musi pozostać zgodne z art. 4 dyrektywy (UE) 2016/680[29].

Ciągłość działania

W niniejszym wniosku umacnia się przepisy dotyczące ciągłości działania zarówno na szczeblu krajowym jak i w odniesieniu do eu-LISA (art. 4, 6, 7 i 15). Przepisy te zapewniają, by SIS nadal działał i był dostępny dla personelu w terenie nawet wówczas, gdy wystąpią problemy mające wpływ na system.

Jakość danych

We wniosku utrzymuje się zasadę, zgodnie z którą państwo członkowskie będące właścicielem danych odpowiada również za prawidłowość danych wprowadzanych do SIS (art. 39). Należy jednak zapewnić centralny mechanizm zarządzany przez eu-LISA, dzięki któremu państwa członkowskie będą mogły regularnie przeprowadzać przegląd wpisów, w przypadku których pola danych obowiązkowych mogą budzić wątpliwości co do jakości danych. W art. 15 upoważnia się zatem eu-LISA do sporządzania w regularnych odstępach czasu sprawozdań dotyczących jakości danych dla państw członkowskich. Wykonanie tego zadania może ułatwić korzystanie z repozytorium danych do celów sporządzania sprawozdań statystycznych i sprawozdań dotyczących jakości danych (art. 54). W ramach wymienionych usprawnień uwzględnia się wstępne ustalenia sformułowane przez grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności.

Fotografie, wizerunki twarzy, dane daktyloskopijne i profile DNA

Możliwość wyszukiwania danych w oparciu o odciski palców w celu ustalenia tożsamości danej osoby określono już w art. 22 rozporządzenia (WE) nr 1987/2006 i decyzji Rady 2007/533/WSiSW. Niniejszy wniosek stanowi, że tego rodzaju wyszukiwanie jest obowiązkowe, jeżeli tożsamość danej osoby nie może zostać potwierdzona w żaden inny sposób. Obecnie wizerunków twarzy nie można wykorzystywać jako podstawowego kryterium wyszukiwania – mogą one być wykorzystywane wyłącznie w celu potwierdzenia

[29] 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, oraz w sprawie swobodnego przepływu takich danych (Dz.U. L 119 z 4.5.2016, s. 89).

tożsamości danej osoby po przeprowadzeniu wyszukania alfanumerycznego. Ponadto zmiany art. 22 i 28 obejmują przepisy dotyczące wykorzystania obrazów twarzy, fotografii i odcisków dłoni do wyszukiwania w systemie i identyfikacji osób, kiedy stanie się to technicznie możliwe. Daktyloskopia to nauka wykorzystująca odciski palców jako metodę identyfikacji. Specjaliści w dziedzinie daktyloskopii uznają, że, tak jak odciski palców, odciski dłoni są unikalne i zawierają punkty odniesienia, które umożliwiają dokładne i rozstrzygające porównanie. Do celów ustalenia tożsamości danej osoby odciski dłoni można wykorzystywać w ten sam sposób co odciski palców. Od wielu lat policja wraz z pobieraniem dziesięciu odbitek płaskich i dziesięciu odbitek przetoczonych pobiera odciski dłoni. Głównym zastosowaniem odcisków dłoni jest zidentyfikowanie danej osoby, która celowo albo niezamierzenie uszkodziła opuszki palców. Niszczenie opuszków palców może stanowić próbę uniknięcia identyfikacji lub pobrania odcisków palców bądź może wynikać z uszkodzenia w wyniku wypadku lub ciężkiej pracy fizycznej. W toku dyskusji na temat zasad technicznych SIS państwa członkowskie poinformowały o istotnym sukcesie systemu automatycznej identyfikacji daktyloskopijnej (AFIS) pod względem identyfikacji nielegalnych migrantów, którzy celowo niszczyli swoje opuszki palców, usiłując uniknąć identyfikacji. Pobranie odcisków dłoni umożliwiło władzom państwa członkowskiego późniejszą identyfikację.

Wykorzystanie wizerunków twarzy do celu identyfikacji zagwarantuje większą zgodność między SIS a proponowanym systemem wjazdu/wyjazdu UE, bramkami elektronicznymi i punktami samoobsługi. Stosowanie tej funkcji będzie ograniczone do zwykłych przejść granicznych.

Dostęp organów do SIS – użytkownicy instytucjonalni

Niniejsza podsekcja ma na celu przedstawienie nowych elementów dotyczących praw dostępu do SIS w odniesieniu do agencji UE (użytkownicy instytucjonalni). Nie wprowadzano zmian do praw dostępu właściwych organów krajowych.

Dostęp do SIS i potrzebnych danych w SIS mają: Europol (art. 30) i Europejska Agencja Straży Granicznej i Przybrzeżnej oraz jej zespoły, zespoły składające się z personelu realizującego zadania w dziedzinie powrotów oraz członkowie zespołu wspierającego zarządzanie migracjami, a także jednostka centralna ETIAS w ramach Agencji (art. 31 i 32). Wprowadza się odpowiednie zabezpieczenia w celu zapewnienia, aby dane w systemie były odpowiednio chronione (czemu służą również przepisy art. 33, w których wymaga się, aby organy te miały dostęp wyłącznie do danych, których potrzebują do celów wykonywania powierzonych im zadań).

W ramach tego rodzaju zmian rozszerza się dostęp Europolu do SIS, tak aby miał on dostęp również do wpisów dotyczących odmowy wjazdu, co ma zagwarantować najlepsze wykorzystanie systemu przez Europol do celów wykonywania powierzonych mu zadań, a także dodaje się nowe przepisy gwarantujące możliwość uzyskania dostępu do systemu przez Europejską Agencję Straży Granicznej i Przybrzeżnej i jej zespoły w toku różnego rodzaju prowadzonych operacji w granicach powierzonych im uprawnień w ramach pomocy państwom członkowskim. Ponadto na podstawie wniosku Komisji dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)[30] jednostka centralna ETIAS

[30] COM(2016) 731 final.

Europejskiej Agencji Straży Granicznej i Przybrzeżnej będzie weryfikować w SIS za pomocą ETIAS, czy w SIS istnieje wpis dotyczący danego obywatela państwa trzeciego ubiegającego się o zezwolenie na podróż. W tym celu jednostka centralna ETIAS będzie miała również dostęp do SIS[31].

Zgodnie z art. 29 ust. 3 krajowe organy wizowe również mogą, w ramach wykonywania swoich zadań, mieć dostęp do wpisów dotyczących dokumentów dokonanych zgodnie z rozporządzeniem 2008/... w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych.

Umożliwi to tym organom uzyskanie dostępu do SIS i danych SIS, których potrzebują do wykonywania swoich zadań, a jednocześnie wprowadzi odpowiednie zabezpieczenia w celu zapewnienia, aby dane w systemie były odpowiednio chronione (czemu służą również przepisy art. 35, w których wymaga się, aby organy te miały dostęp wyłącznie do danych, których potrzebują do celów wykonywania powierzonych im zadań).

Odmowa wjazdu i pobytu

Obecnie zgodnie z art. 24 ust. 3 rozporządzenia SIS II państwo członkowskie może dokonać w SIS wpisu dotyczącego osoby objętej zakazem wjazdu z uwagi na naruszenie krajowych przepisów migracyjnych. Zmieniony art. 24 ust. 3 wymaga dokonania wpisu w SIS we wszystkich przypadkach wydania zakazu wjazdu dotyczącego nielegalnie przebywającego obywatela państwa trzeciego zgodnie z przepisami zgodnymi z dyrektywą 2008/115/WE. Określa też terminy i warunki dokonania takiego wpisu po opuszczeniu przez obywatela państwa trzeciego terytorium państw członkowskich zgodnie z zobowiązaniem do powrotu. Przepis ten wprowadzono, aby uniknąć sytuacji, w której zakazy wjazdu figurują w SIS, podczas gdy dany obywatel państwa trzeciego nadal przebywa na terytorium UE. Ponieważ zakazy wjazdu zakazują ponownego wjazdu na terytorium państw członkowskich, mogą wejść w życie dopiero po powrocie obywateli państw trzecich, których to obywateli dotyczą. Jednocześnie państwa członkowskie powinny podjąć wszelkie niezbędne kroki w celu zapewnienia, by między momentem powrotu a aktywowaniem w SIS wpisu dotyczącego zakazu wjazdu i pobytu nie wystąpiła luka czasowa.

Niniejszy wniosek jest ściśle powiązany z wnioskiem Komisji[32] dotyczącym użytkowania SIS do celów powrotu nielegalnie przebywających obywateli państw trzecich, określającym warunki i procedury dokonywania w SIS wpisów dotyczących decyzji nakazujących powrót. Wniosek ten obejmuje mechanizm monitorowania, czy obywatel państwa trzeciego, którego dotyczy decyzja nakazująca powrót, faktycznie opuścił terytorium UE, oraz mechanizm ostrzegawczy w przypadku niewykonania decyzji. Artykuł 26 ustanawia procedurę konsultacji, którą państwa członkowskie muszą stosować, kiedy mają do czynienia z wpisami dotyczącymi zakazu wjazdu i pobytu kolidującymi z decyzjami innych państw członkowskich (na przykład z ważnymi dokumentami pobytowymi) – lub kiedy chcą dokonać takich wpisów. Takie zasady powinny zapobiegać wystąpieniu sprzecznych instrukcji, które mogą wynikać z takich sytuacji, i rozstrzygać takie kwestie, jednocześnie oferując użytkownikom końcowym jasne wytyczne co do działań, które należy podjąć, a także wskazując organom państw członkowskich, czy należy w takim przypadku usunąć wpis.

---

31 Jednostka centralna ETIAS ma dostęp do art. 24 i 27 niniejszego rozporządzenia.

32 COM (2016)…

Artykuł 27 (dawny art. 26 rozporządzenia (WE) nr 1987/2006) ma na celu wdrożenie systemu sankcji UE dotyczących obywateli państw trzecich, których obejmują ograniczenia dotyczące wjazdu na terytorium UE, zgodnie z art. 29 Traktatu o Unii Europejskiej. Aby umożliwić dokonywanie takich wpisów, konieczne było wprowadzenie wymogów dotyczących minimalnej ilości danych niezbędnych do identyfikacji danej osoby, czyli nazwiska i daty urodzenia. Fakt, że w rozporządzeniu (WE) nr 1987/2006 odstąpiono od wymogu wprowadzania daty urodzenia, spowodował znaczne problemy, gdyż bez daty urodzenia nie można dokonać wpisu w SIS ze względu na zasady techniczne i parametry wyszukiwania w systemie. Ponieważ art. 27 jest niezbędny do wprowadzenia skutecznego systemu sankcji UE, wymóg proporcjonalności nie ma w tym kontekście zastosowania.

Aby zapewnić większą spójność z dyrektywą 2008/115/WE, terminologia stosowana w odniesieniu do celów wpisu („zakaz wjazdu i pobytu") została dostosowana do sformułowań używanych w tej dyrektywie.

Rozróżnianie osób o podobnych cechach

Aby zapewnić, że dane są przetwarzane i przechowywane w odpowiedni sposób, oraz ograniczyć ryzyko powielania i błędnej identyfikacji, art. 41 określa procedurę, którą należy zastosować, gdy przy dokonywaniu nowego wpisu wydaje się, że w SIS istnieje już wpis o podobnych cechach.

Ochrona i bezpieczeństwo danych

W niniejszym wniosku wyjaśnia się kwestię odpowiedzialności w zakresie zapobiegania zdarzeniom, które mogą mieć wpływ na bezpieczeństwo lub integralność infrastruktury SIS, danych w SIS lub informacji uzupełniających, w zakresie zgłaszania tego rodzaju zdarzeń oraz reagowania na tego rodzaju zdarzenia (art. 10, 16 i 40).

Artykuł 12 zawiera przepisy dotyczące przechowywania i wyszukiwania rejestrów obejmujących historię wpisów.

W art. 15 ust. 3 zachowuje się art. 15 ust. 3 rozporządzenia (WE) nr 1987/2006, który stanowi, że Komisja pozostaje odpowiedzialna za zarządzanie umowami w zakresie infrastruktury łączności, w tym zadania związane z wykonaniem budżetu oraz zakupy i odnawianie. Zadania te zostaną powierzone eu-LISA w drugim pakiecie wniosków dotyczących SIS w czerwcu 2017 r.

W art. 21 rozszerza się wymóg, zgodnie z którym przed dokonaniem wpisu państwa członkowskie powinny rozważyć proporcjonalność, tak aby wymóg ten miał również zastosowanie do decyzji w sprawie rozszerzenia okresu ważności wpisu. Jako nowy element w art. 24 ust. 2 lit. c) wymaga się jednak, aby państwa członkowskie tworzyły wpis we wszystkich okolicznościach w odniesieniu do osób, których działalność jest objęta zakresem stosowania art. 1, 2, 3 i 4 decyzji ramowej Rady 2002/475/WSiSW w sprawie zwalczania terroryzmu.

<u>Kategorie danych i przetwarzanie danych</u>

Aby zapewnić użytkownikom końcowym bardziej wyczerpujące i dokładniejsze informacje, by ułatwić i przyspieszyć wymagane działania oraz umożliwić skuteczniejszą identyfikację osoby, której dotyczy wpis, w niniejszym wniosku rozszerza się wykaz informacji (art. 20),

które można przechowywać na temat osób, w odniesieniu do których dokonano wpisu, tak aby obejmował on również następujące informacje:

- informacje, czy dana osoba uczestniczy w działaniu, o którym mowa w art. 1, 2, 3 i 4 decyzji ramowej Rady 2002/475/WSiSW;
- informacje, czy wpis ma związek z obywatelem UE lub inną osobą, która korzysta z prawa swobodnego przemieszczania się równoważnego z prawem obywateli Unii Europejskiej;
- informacje, czy decyzję o odmowie wjazdu podjęto na podstawie przepisów art. 24 lub art. 27;
- rodzaj przestępstwa (w przypadku wpisów dokonanych zgodnie z art. 24 ust. 2);
- szczegółowe informacje na temat dokumentu tożsamości lub dokumentu podróży danej osoby;
- kolorową kopię dokumentu tożsamości lub dokumentu podróży danej osoby;
- fotografie i wizerunki twarzy;
- odciski palców i dłoni.

Posiadanie odpowiednich danych jest niezbędne, aby zapewnić precyzyjną identyfikację osoby kontrolowanej na przejściu granicznym, osoby, która podlega kontroli wewnętrznej, albo osoby ubiegającej się o zezwolenie na pobyt. Błędna identyfikacja może doprowadzić do naruszenia praw podstawowych, a także do sytuacji, w której nie można podjąć odpowiednich działań następczych, gdyż brak jest wiedzy o istnieniu lub treści wpisu.

Jeżeli chodzi o informacje będące podstawą decyzji, można wyróżnić cztery przyczyny: wcześniejszy wyrok skazujący, o którym mowa w art. 24 ust. 2 lit. a); poważne zagrożenie bezpieczeństwa, o którym mowa w art. 24 ust. 2 lit. b); zakaz wjazdu, o którym mowa w art. 24 ust. 3; oraz środek ograniczający, o którym mowa w art. 27. Aby zapewnić podjęcie odpowiednich działań w przypadku trafienia, należy także określić, czy wpis ma związek z obywatelem UE lub inną osobą, która korzysta z prawa swobodnego przemieszczania się równoważnego z prawem obywateli Unii Europejskiej. Posiadanie odpowiednich danych jest niezbędne, aby zapewnić precyzyjną identyfikację osoby kontrolowanej na przejściu granicznym, osoby, która podlega kontroli wewnętrznej, albo osoby ubiegającej się o zezwolenie na pobyt. Błędna identyfikacja może doprowadzić do naruszenia praw podstawowych, a także do sytuacji, w której nie można podjąć odpowiednich działań następczych, gdyż brak jest wiedzy o istnieniu lub treści wpisu.

W art. 42 rozszerzono też wykaz danych osobowych, jakie można wprowadzać do SIS i przetwarzać w tym systemie w celu rozwiązania problemów związanych z błędną identyfikacją osób, gdyż więcej danych ułatwia określenie pokrzywdzonego i sprawcy przestępstwa przywłaszczenia tożsamości. Rozszerzenie zakresu tego przepisu nie stanowi zagrożenia, gdyż wszystkie te dane można wprowadzić wyłącznie za zgodą ofiary przestępstwa przywłaszczenia tożsamości. Obecnie dane te obejmą również:

- wizerunek twarzy;

- odciski dłoni;
- dane z dokumentów tożsamości;
- adres pokrzywdzonego;
- imiona i nazwiska rodziców pokrzywdzonego.

W art. 20 przewiduje się bardziej szczegółowe informacje we wpisach. Informacje te obejmują kategorie odnoszące się do przyczyn odmowy wjazdu i pobytu oraz szczegółowe dane z dokumentów tożsamości osób, których dane dotyczą. Rozszerzone informacje pozwalają na lepszą identyfikację danej osoby oraz na podjęcie bardziej świadomej decyzji przez użytkowników końcowych. W celu ochrony użytkowników końcowych prowadzących kontrole SIS wskaże także, czy osoba, wobec której dokonano wpisu, zalicza się do jednej z kategorii określonych w art. 1, 2, 3 i 4 decyzji ramowej Rady 2002/475/WSiSW w sprawie zwalczania terroryzmu[33].

We wniosku wyraźnie stwierdzono, że państwa członkowskie nie mogą kopiować danych wprowadzonych przez inne państwo członkowskie do innych krajowych plików danych (art. 37).

Przechowywanie

W art. 34 przedstawiono ramy czasowe przeglądu wpisów. Maksymalny okres przechowywania wpisów dotyczących odmowy wjazdu i pobytu dostosowano do maksymalnej długości zakazów wjazdu wydanych zgodnie z art. 11 dyrektywy 2008/115/WE. Maksymalny okres przechowywania wyniesie zatem 5 lat. Państwa członkowskie mogą jednak ustanowić krótsze okresy.

Usuwanie

W art. 35 określono okoliczności, w których należy usunąć wpisy w celu zapewnienia większej harmonizacji praktyk krajowych w tej dziedzinie. W art. 35 określono szczególne przepisy umożliwiające personelowi biura SIRENE aktywne usuwanie wpisów, które nie są już potrzebne, w przypadku braku odpowiedzi ze strony właściwych organów.

Prawo dostępu do danych, korekty nieścisłości oraz usunięcia danych przechowywanych niezgodnie z prawem przysługujące osobom, których dane dotyczą

Szczegółowe przepisy dotyczące praw osób, których dane dotyczą, pozostają niezmienione, ponieważ obowiązujące przepisy zapewniają już wysoki poziom ochrony i są zgodne z rozporządzeniem (UE) 2016/679[34] i dyrektywą 2016/680[35]. Oprócz tego w art. 48 określono

[33] Decyzja ramowa Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. L 164 z 22.6.2002, s. 3).

[34] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

[35] 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

okoliczności, w których państwa członkowskie mogą podjąć decyzję o nieprzekazywaniu informacji osobom, których dane dotyczą. Może się tak stać w wyniku jednej z przyczyn wymienionych w tym artykule, przy czym takie działanie musi być proporcjonalne i konieczne oraz zgodne z prawem krajowym.

Dane statystyczne

Aby śledzić sposób działania środków zaradczych, w art. 49 przewidziano standardowy system statystyczny zapewniający roczne sprawozdania na temat:

- liczby wniosków o uzyskanie dostępu złożonych przez osoby, których dane dotyczą;
- liczby wniosków dotyczących korekty nieścisłości oraz usunięcia danych wprowadzonych niezgodnie z prawem;
- liczby spraw rozpatrywanych przez sąd;
- liczby spraw, w których sąd orzekł na korzyść wnioskodawcy; oraz
- liczby uwag dotyczących przypadków wzajemnego uznawania orzeczeń kończących postępowanie w sprawie wydanych przez sądy lub organy innych państw członkowskich w odniesieniu do wpisów utworzonych przez państwo dokonujące wpisu.

Monitorowanie i statystyka

W art. 54 przedstawiono ustalenia, które należy wprowadzić w celu zapewnienia prawidłowego monitorowania i funkcjonowania SIS zgodnie z jego celami. Aby to osiągnąć, należy zobowiązać eu-LISA do dostarczania dziennych, miesięcznych i rocznych danych statystycznych na temat sposobu wykorzystania systemu.

Artykuł 54 ust. 5 wymaga, by eu-LISA przekazywała państwom członkowskim, Komisji, Europolowi i Europejskiej Agencji Straży Granicznej i Przybrzeżnej opracowane przez siebie sprawozdania statystyczne, oraz umożliwia Komisji żądanie przedstawienia dodatkowych sprawozdań statystycznych i sprawozdań dotyczących jakości danych odnoszących się do komunikacji SIS i SIRENE.

W art. 54 ust. 6 przewiduje się utworzenie i prowadzenie centralnego repozytorium danych w ramach prowadzonych przez eu-LISA prac nad monitorowaniem funkcjonowania SIS. Pozwoli to upoważnionym pracownikom państw członkowskich, Komisji, Europolu i Europejskiej Agencji Straży Granicznej i Przybrzeżnej uzyskać dostęp do danych wymienionych w art. 54 ust. 3 w celu sporządzenia wymaganych statystyk.

ścigania czynów zabronionych i wykonywania kar, oraz w sprawie swobodnego przepływu takich danych (Dz.U. L 119 z 4.5.2016, s. 89).

2016/0408 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmieniające rozporządzenie (UE) nr 515/2014 i uchylające rozporządzenie (WE) nr 1987/2006

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 77 ust. 2 lit. b) i d) oraz art. 79 ust. 2 lit. c),

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) System Informacyjny Schengen (SIS) stanowi zasadniczy instrument stosowania postanowień dorobku Schengen, który włączony został w ramy Unii Europejskiej. SIS jest jednym z głównych środków uzupełniających, który przyczynia się do utrzymania wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej poprzez wspomaganie współpracy operacyjnej straży granicznej, policji, organów celnych, innych organów ścigania i organów sądowniczych w sprawach karnych oraz organów imigracyjnych.

(2) SIS został ustanowiony na mocy postanowień tytułu IV konwencji wykonawczej z dnia 19 czerwca 1990 r. do układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach[36] („konwencja z Schengen”).Opracowanie systemu SIS drugiej generacji (SIS II) powierzono Komisji na mocy rozporządzenia Rady (WE) nr 2424/2001[37] i decyzji Rady 2001/886/WSiSW[38] (SIS); został on utworzony na mocy rozporządzenia (WE) nr 1987/2006[39] i decyzji Rady 2007/533/WSiSW[40]. SIS II zastąpił SIS, który powstał na mocy konwencji z Schengen.

---

36 Dz.U. L 239 z 22.9.2000, s. 19. Konwencja zmieniona rozporządzeniem (WE) nr 1160/2005 Parlamentu Europejskiego i Rady (Dz.U. L 191 z 22.7.2005, s. 18).

37 Dz.U. L 328 z 13.12.2001, s. 4.

38 Decyzja Rady 2001/886/WSiSW z dnia 6 grudnia 2001 r. w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 328 z 13.12.2001, s. 1).

39 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.U. L 181 z 28.12.2006, s. 4).

(3) Trzy lata po wprowadzeniu SIS II Komisja przeprowadziła ocenę systemu zgodnie z art. 24 ust. 5, art. 43 ust. 5 i art. 50 ust. 5 rozporządzenia (WE) nr 1987/2006 oraz art. 59 i art. 65 ust. 5 decyzji 2007/533/WSiSW. Sprawozdanie z oceny i powiązany dokument roboczy służb Komisji przyjęto w dniu 21 grudnia 2016 r.[41]. Zalecenia zawarte w tych dokumentach powinny znaleźć odzwierciedlenie, w stosownych przypadkach, w niniejszym rozporządzeniu.

(4) Niniejsze rozporządzenie stanowi niezbędną podstawę prawną dla systemu SIS w kwestiach objętych zakresem stosowania rozdziału 2 tytułu V Traktatu o funkcjonowaniu Unii Europejskiej. Rozporządzenie (UE) 2018/... Parlamentu Europejskiego i Rady w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych[42] stanowi niezbędną podstawę prawną dla systemu SIS w kwestiach objętych zakresem stosowania rozdziału 4 i 5 tytułu V Traktatu o funkcjonowaniu Unii Europejskiej.

(5) Fakt, że podstawa prawna SIS składa się z odrębnych aktów, nie narusza zasady, że SIS stanowi i powinien funkcjonować jako jednolity system informacyjny. Niektóre postanowienia tych aktów powinny być zatem identyczne.

(6) Niezbędne jest dokładne określenie przeznaczenia SIS, jego struktury technicznej i finansowania, ustanowienie zasad jego pełnego funkcjonowania i użytkowania oraz określenie zakresów odpowiedzialności, kategorii danych, które będą wprowadzane do systemu, celów, do jakich dane te mają być wprowadzane, kryteriów ich wprowadzania, organów mających prawo dostępu do danych, odesłań do identyfikatorów biometrycznych oraz dalszych zasad przetwarzania danych.

(7) SIS obejmuje system centralny (centralny SIS) oraz systemy krajowe z pełną lub częściową kopią bazy danych SIS. Biorąc pod uwagę, że SIS jest najważniejszym narzędziem wymiany informacji w Europie, konieczne jest zapewnienie jego nieprzerwanego działania na szczeblu centralnym i krajowym. Każde państwo członkowskie powinno zatem utworzyć częściową lub pełną kopię bazy danych SIS oraz system zapasowy.

(8) Należy utrzymać podręcznik określający szczegółowe zasady wymiany informacji uzupełniających dotyczących działań, które zgodnie z wpisami należy podjąć. Organy krajowe w każdym państwie członkowskim (biura SIRENE) powinny zapewnić wymianę takich informacji.

(9) Aby utrzymać skuteczną wymianę informacji uzupełniających dotyczących podjęcia działania określonego we wpisach, należy wzmocnić funkcjonowanie biur SIRENE poprzez określenie wymogów dotyczących dostępnych zasobów, szkoleń

---

40 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. L 205 z 7.8.2007, s. 63).

41 Sprawozdanie 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 oraz towarzyszący mu dokument roboczy służb Komisji.

42 Rozporządzenie (UE) 2018/...

użytkowników i czasu na udzielenie odpowiedzi na pytania nadesłane z innych biur SIRENE.

(10) Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości[43] („Agencja") odpowiada za zarządzanie operacyjne centralnymi komponentami SIS. Aby umożliwić Agencji przeznaczenie niezbędnych zasobów finansowych i osobowych obejmujących wszystkie aspekty zarządzania operacyjnego centralnym SIS, w niniejszym rozporządzeniu należy szczegółowo określić jej zadania, przede wszystkim w odniesieniu do technicznych aspektów wymiany informacji uzupełniających.

(11) Bez uszczerbku dla obowiązku państw członkowskich dotyczącego zapewnienia dokładności danych wprowadzanych do SIS, Agencja powinna być odpowiedzialna za podniesienie jakości danych poprzez wprowadzenie centralnego narzędzia monitorowania jakości danych oraz za przekazywanie państwom członkowskim sprawozdań w regularnych odstępach czasu.

(12) Aby umożliwić lepsze monitorowanie wykorzystania SIS do analizowania tendencji związanych z presją migracyjną i zarządzaniem granicami, Agencja powinna mieć możliwość rozwijania nowoczesnych zdolności w zakresie prowadzenia sprawozdawczości statystycznej wobec państw członkowskich, Komisji, Europolu i Europejskiej Agencji Straży Granicznej i Przybrzeżnej bez naruszania integralności danych. Należy zatem utworzyć centralne repozytorium statystyczne. Żadna z opracowanych statystyk nie powinna zawierać danych osobowych.

(13) SIS powinien zawierać dodatkowe kategorie danych, aby umożliwić użytkownikom końcowym bezzwłoczne podejmowanie świadomych decyzji na podstawie wpisu. W związku z tym wpisy do celów odmowy wjazdu powinny zawierać informacje dotyczące decyzji, na której opiera się wpis. W celu ułatwienia identyfikacji i wykrycia wielorakich tożsamości wpis powinien ponadto zawierać odniesienie do dokumentu tożsamości lub numeru i kopii takiego dokumentu, jeżeli jest dostępny.

(14) SIS nie powinien przechowywać żadnych danych wykorzystywanych do wyszukiwania, z wyjątkiem rejestrów służących do sprawdzenia, czy dane wyszukiwanie jest dopuszczalne, do monitorowania dopuszczalności przetwarzania danych, autokontroli oraz zapewniania należytego działania N.SIS, integralności danych i bezpieczeństwa.

(15) SIS powinien umożliwiać przetwarzanie danych biometrycznych, aby ułatwić niezawodną identyfikację osób, których dotyczy wpis. Równocześnie SIS powinien pozwalać na przetwarzanie danych dotyczących osób, które są ofiarami przywłaszczenia tożsamości (w celu uniknięcia niedogodności powodowanych błędną identyfikacją tych osób), pod warunkiem zastosowania odpowiednich zabezpieczeń, a zwłaszcza za zgodą danej osoby i przy ścisłym ograniczeniu celów, w których takie dane mogą być zgodnie z prawem przetwarzane.

---

[43] Ustanowiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. ustanawiającym Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz.U. L 286 z 1.11.2011, s. 1).

(16) Państwa członkowskie powinny dokonać niezbędnych ustaleń technicznych, tak aby za każdym razem użytkownicy końcowi byli uprawnieni do przeprowadzenia wyszukiwania w krajowej bazie danych policji lub bazie imigracyjnej oraz do równoległego prowadzenia wyszukiwania w SIS zgodnie z art. 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680[44]. Dzięki temu SIS powinien działać jako główny środek uzupełniający na obszarze bez kontroli na granicach wewnętrznych i lepiej uwzględniać transgraniczny wymiar przestępczości i mobilności przestępców.

(17) W niniejszym rozporządzeniu należy określić warunki korzystania z danych daktyloskopijnych i wizerunków twarzy w celach identyfikacyjnych. Korzystanie z wizerunków twarzy w celach identyfikacyjnych w SIS powinno także pomóc w zapewnieniu spójności procedur kontroli granicznej, gdy identyfikacja i weryfikacja tożsamości wymaga wykorzystania danych daktyloskopijnych i wizerunków twarzy. Wyszukiwanie na podstawie danych daktyloskopijnych powinno być obowiązkowe, jeżeli istnieją jakiekolwiek wątpliwości co do tożsamości danej osoby. Wizerunki twarzy do celów identyfikacyjnych powinny być stosowane tylko w kontekście regularnych kontroli granicznych w punktach samoobsługi i przy bramkach elektronicznych.

(18) Należy umożliwić porównanie linii papilarnych znalezionych na miejscu przestępstwa z danymi daktyloskopijnymi przechowywanymi w SIS, jeżeli z bardzo dużą dozą prawdopodobieństwa można ustalić, że należą one do sprawcy poważnego przestępstwa lub przestępstwa terrorystycznego. Za „poważne przestępstwo" należy uznać przestępstwa wymienione w decyzji ramowej Rady 2002/584/WSiSW[45], zaś za „przestępstwa terrorystyczne" uznaje się przestępstwa w rozumieniu prawa krajowego, o których mowa w decyzji ramowej Rady 2002/475/WSiSW[46].

(19) Państwa członkowskie powinny mieć możliwość tworzenia w SIS odsyłaczy do innych wpisów. Utworzenie przez państwo członkowskie odsyłacza do co najmniej jednego innego wpisu nie powinno mieć wpływu na działanie, jakie należy podjąć, ani na okres przechowywania tych wpisów, ani na prawa dostępu do nich.

(20) Większy stopień skuteczności, harmonizacji i spójności można osiągnąć poprzez wprowadzenie obowiązku wpisywania do SIS wszystkich zakazów wjazdu wydanych przez właściwe organy państw członkowskich zgodnie z procedurami zgodnymi z dyrektywą 2008/115/WE[47] oraz ustanowienie wspólnych zasad dotyczących dokonywania takich wpisów w następstwie powrotu nielegalnie przebywającego

---

44 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

45 Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. L 190 z 18.7.2002, s. 1).

46 Decyzja ramowa Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. L 164 z 22.6.2002, s. 3).

47 Dyrektywa Parlamentu Europejskiego i Rady 2008/115/WE z dnia 16 grudnia 2008 r. w sprawie wspólnych norm i procedur stosowanych przez państwa członkowskie w odniesieniu do powrotów nielegalnie przebywających obywateli państw trzecich (Dz.U. L 348 z 24.12.2008, s. 98).

obywatela państwa trzeciego. Państwa członkowskie powinny podjąć wszelkie niezbędne kroki w celu zapewnienia, by między wyjazdem obywatela państwa trzeciego a aktywowaniem w SIS wpisu nie wystąpiła luka czasowa. Powinno to zapewnić skuteczne egzekwowanie zakazów wjazdu na zewnętrznych przejściach granicznych, faktycznie uniemożliwiając ponowny wjazd do strefy Schengen.

(21) Niniejsze rozporządzenie powinno określać bezwzględnie obowiązujące przepisy w sprawie konsultacji organów krajowych w przypadku, gdy obywatel państwa trzeciego posiada lub może uzyskać ważny dokument pobytowy lub inne zezwolenie na pobyt lub prawo pobytu przyznane w jednym państwie członkowskim, a inne państwo członkowskie zamierza dokonać lub już dokonało wpisu dotyczącego zakazu wjazdu i pobytu obejmującego danego obywatela państwa trzeciego. W takich sytuacjach straż graniczna, policja i organy imigracyjne miewają duże wątpliwości. Należy zatem ustanowić obowiązkowe ramy prawne szybkiej konsultacji z konkretnymi wynikami, aby uniknąć sytuacji, w której osoba stanowiąca zagrożenie może wjechać do strefy Schengen.

(22) Niniejsze rozporządzenie nie powinno naruszać stosowania dyrektywy 2004/38/WE[48].

(23) Wpisów nie należy przechowywać w SIS dłużej, niż jest to konieczne do osiągnięcia celów, w jakich zostały dodane. Aby ograniczyć obciążenie administracyjne organów zaangażowanych w przetwarzanie danych dotyczących osób fizycznych do różnych celów, należy dostosować maksymalny okres przechowywania wpisów dotyczących odmowy wjazdu i pobytu do maksymalnej długości zakazów wjazdu wydanych zgodnie z procedurami zgodnymi z dyrektywą 2008/115/WE. Okres przechowywania wpisów dotyczących osób powinien zatem wynosić maksymalnie pięć lat. Obowiązuje ogólna zasada, że wpisy dotyczące osób powinny być automatycznie usuwane z SIS po upływie pięciu lat. Decyzje o zachowaniu wpisów powinny być podejmowane na podstawie wszechstronnej indywidualnej oceny. Państwa członkowskie powinny w ciągu określonego okresu zweryfikować wpisy dotyczące osób, a ponadto prowadzić statystyki dotyczące liczby wpisów dotyczących osób, których okres przechowywania został przedłużony.

(24) Wprowadzenie i wydłużenie terminu ważności wpisu w SIS powinno podlegać wymogowi zachowania niezbędnej proporcjonalności oraz zbadaniu, czy konkretny przypadek jest adekwatny, odpowiedni i wystarczająco ważny, aby dokonać wpisu w SIS. W przypadku przestępstw, o których mowa w art. 1, 2, 3 i 4 decyzji ramowej Rady 2002/475/WSiSW[49] w sprawie zwalczania terroryzmu, zawsze należy dokonywać wpisu dotyczącego obywateli państw trzecich do celów odmowy wjazdu i pobytu, uwzględniając wysoki poziom zagrożenia i ogólne negatywne skutki, jakie takie działania mogą spowodować.

(25) Kluczowe znaczenie ma integralność danych SIS. Należy zatem zapewnić odpowiednie zabezpieczenia podczas przetwarzania danych SIS na szczeblu centralnym i krajowym w celu zapewnienia pełnego bezpieczeństwa danych. Organy

---

48 Dyrektywa 2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium państw członkowskich (Dz.U. L 158 z 30.4.2004, s. 77).

49 Decyzja ramowa Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. L 164 z 22.6.2002, s. 3).

uczestniczące w przetwarzaniu danych powinny być objęte wymogami bezpieczeństwa określonymi w niniejszym rozporządzeniu i podlegać jednolitej procedurze zgłaszania incydentów.

(26) Dane przetwarzane w SIS na użytek niniejszego rozporządzenia nie powinny być przekazywane ani udostępniane państwom trzecim ani organizacjom międzynarodowym.

(27) Aby zwiększyć skuteczność prac organów imigracyjnych dotyczących podejmowania decyzji w sprawie prawa obywateli państw trzecich do wjazdu i pobytu na terytorium państw członkowskich oraz powrotu nielegalnie przebywających obywateli państw trzecich, należy przyznać tym organom dostęp do SIS na mocy niniejszego rozporządzenia.

(28) Rozporządzenie (UE) 2016/679[50] powinno mieć zastosowanie do przetwarzania danych osobowych przez organy państw członkowskich na mocy niniejszego rozporządzenia, gdy dyrektywa (UE) 2016/680[51] nie ma zastosowania. Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady[52] powinno mieć zastosowanie do przetwarzania danych osobowych przez instytucje i organy unijne podczas wykonywania przez nie swoich obowiązków na mocy niniejszego rozporządzenia. W razie potrzeby przepisy określone w dyrektywie (UE) 2016/680, rozporządzeniu (UE) 2016/679 i rozporządzeniu (WE) nr 45/2001 powinny zostać doprecyzowane w niniejszym rozporządzeniu. W odniesieniu do przetwarzania danych osobowych przez Europol zastosowanie ma rozporządzenie (UE) 2016/794 w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania[53] (rozporządzenie w sprawie Europolu).

(29) Odpowiednie przepisy Regulaminu pracowniczego urzędników i warunków zatrudnienia innych pracowników Unii Europejskiej dotyczące poufności powinny mieć zastosowanie do urzędników lub innych pracowników, którzy są zatrudnieni i pracują przy SIS.

(30) Zarówno państwa członkowskie, jak i Agencja powinny utrzymać plany bezpieczeństwa, które w praktyce ułatwią realizację wymogów bezpieczeństwa, oraz powinny ze sobą współpracować, tak aby rozpatrywać kwestie bezpieczeństwa ze wspólnego punktu widzenia.

---

50 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

51 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, oraz w sprawie swobodnego przepływu takich danych (Dz.U. L 119 z 4.5.2016, s. 89).

52 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

53 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 2009/968/WSiSW (Dz.U. L 135 z 25.5.2016, s. 53).

(31) Niezależne krajowe organy nadzorcze powinny monitorować zgodność z prawem przetwarzania danych osobowych przez państwa członkowskie w odniesieniu do niniejszego rozporządzenia. Należy ustanowić prawa dostępu do danych osobowych przechowywanych w SIS, ich poprawiania i usuwania przysługujące osobom, których dane dotyczą, oraz późniejsze środki zaradcze możliwe do uzyskania przed sądami krajowymi i wzajemne uznawanie orzeczeń sądowych. Właściwe jest zatem wymaganie rocznych danych statystycznych od państw członkowskich.

(32) Organy nadzorcze powinny zapewnić, aby co najmniej co cztery lata przeprowadzany był audyt operacji przetwarzania danych w ramach ich N.SIS zgodnie z międzynarodowymi standardami audytu. Audyt powinny prowadzać organy nadzorcze lub krajowe organy nadzorcze powinny bezpośrednio zlecić przeprowadzenie audytu niezależnemu audytorowi ds. ochrony danych. Niezależny audytor powinien pozostawać pod nadzorem krajowych organów nadzorczych i na odpowiedzialność tych organów, które w związku z tym powinny same zlecić przeprowadzenie audytu i zapewnić jasno określony cel, zakres i metodykę audytu oraz wytyczne i nadzór dotyczący audytu i jego wyników końcowych.

(33) Rozporządzenie (UE) 2016/794 (rozporządzenie w sprawie Europolu) stanowi, że Europol wspiera i wzmacnia działania prowadzone przez właściwe organy państw członkowskich oraz współpracę między tymi organami w zakresie zwalczania terroryzmu i poważnych przestępstw oraz zapewnia analizę i oceny zagrożeń. Aby ułatwić Europolowi wykonywanie jego zadań, w szczególności w ramach Europejskiego Centrum Zwalczania Przemytu Migrantów, należy przyznać Europolowi dostęp do tej kategorii wpisów określonych w niniejszym rozporządzeniu. Europejskie Centrum Zwalczania Przemytu Migrantów działające przy Europolu odgrywa ważną rolę strategiczną w zwalczaniu ułatwiania nielegalnej migracji, należy więc zapewnić mu dostęp do wpisów dotyczących osób, którym odmówiono wjazdu lub pobytu na terytorium państwa członkowskiego z powodów naruszenia przepisów prawa karnego lub nieprzestrzegania warunków dotyczących wjazdu i pobytu.

(34) Aby zniwelować luki w informacjach udostępnianych na temat terroryzmu, w szczególności na temat zagranicznych bojowników terrorystycznych – w przypadku gdy niezbędne jest monitorowanie sposobu, w jaki się przemieszczają – państwa członkowskie powinny udostępniać Europolowi informacje na temat działań związanych z terroryzmem równolegle z wprowadzaniem wpisów do SIS, a także informacje o trafieniach i powiązane informacje. Powinno to umożliwić Europejskiemu Centrum ds. Zwalczania Terroryzmu działającemu przy Europolu sprawdzenie, czy istnieją jakiekolwiek dodatkowe informacje kontekstowe dostępne w bazach danych Europolu oraz dostarczenie wysokiej jakości analizy przyczyniającej się do zakłócenia sieci terrorystycznej i, w miarę możliwości, zapobiegającej jej atakom.

(35) Konieczne jest również określenie jasnych zasad dla Europolu dotyczących przetwarzania i pobierania danych SIS w celu umożliwienia kompleksowego wykorzystania SIS, pod warunkiem że normy ochrony danych są przestrzegane zgodnie z niniejszym rozporządzeniem i rozporządzeniem (UE) 2016/794. Jeżeli w wyniku wyszukiwania w SIS Europol wykryje istnienie wpisu dokonanego przez państwo członkowskie, wówczas nie może podjąć wymaganego działania. Dlatego należy poinformować dane państwo członkowskie, umożliwiając mu podjęcie odpowiednich działań następczych.

(36) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624[54] stanowi, że na potrzeby niniejszego rozporządzenia przyjmujące państwo członkowskie upoważnia członków zespołów Europejskiej Straży Granicznej i Przybrzeżnej lub zespołów składających się z personelu realizującego zadania w dziedzinie powrotów, rozmieszczonych przez Europejską Agencję Straży Granicznej i Przybrzeżnej, do korzystania z europejskich baz danych, w przypadku gdy konsultacje te są niezbędne do realizacji celów operacyjnych określonych w planie operacyjnym w odniesieniu do odpraw granicznych, ochrony granic i powrotów. Inne istotne agencje unijne, w szczególności Europejski Urząd Wsparcia w dziedzinie Azylu i Europol, również mogą rozmieszczać – w ramach zespołów wspierających zarządzanie migracjami – swoich ekspertów, którzy nie są pracownikami tych agencji unijnych. Celem rozmieszczenia zespołów Europejskiej Straży Granicznej i Przybrzeżnej, zespołów składających się z personelu realizującego zadania w dziedzinie powrotów oraz zespołów wspierających zarządzanie migracjami jest zapewnienie wzmocnienia technicznego i operacyjnego wnioskujących państw członkowskich, zwłaszcza tych zmagających się z nieproporcjonalnymi wyzwaniami migracyjnymi. Realizacja zadań przypisanych zespołom Europejskiej Straży Granicznej i Przybrzeżnej, zespołom składającym się z personelu realizującego zadania w dziedzinie powrotów oraz zespołom wspierającym zarządzanie migracjami wymaga dostępu do SIS za pośrednictwem interfejsu technicznego łączącego Europejską Agencję Straży Granicznej i Przybrzeżnej z centralnym SIS. Jeżeli w wyniku wyszukiwania w SIS zespoły pracowników wykryją istnienie wpisu dokonanego przez państwo członkowskie, wówczas członek zespołu lub personelu nie może podjąć wymaganego działania, chyba że został do tego upoważniony przez przyjmujące państwo członkowskie. Dlatego należy poinformować dane państwa członkowskie, umożliwiając im podjęcie odpowiednich działań następczych.

(37) Zgodnie z rozporządzeniem (UE) 2016/1624 Europejska Agencja Straży Granicznej i Przybrzeżnej przygotowuje analizy ryzyka. Analizy te obejmują wszelkie aspekty istotne dla europejskiego zintegrowanego zarządzania granicami, w szczególności zagrożenia, które mogą wpłynąć na funkcjonowanie lub bezpieczeństwo granic zewnętrznych. Wpisy dokonane w SIS zgodnie z niniejszym rozporządzeniem, w szczególności wpisy dotyczące zakazu wjazdu i pobytu, stanowią istotne informacje do oceny ewentualnych zagrożeń, które mogą mieć wpływ na granice zewnętrzne; wpisy te powinny w związku z tym być dostępne do celów analizy ryzyka, którą musi przygotowywać Europejska Agencja Straży Granicznej i Przybrzeżnej. Realizacja zadań przypisanych Europejskiej Agencji Straży Granicznej i Przybrzeżnej związanych z analizą ryzyka wymaga dostępu do SIS. Ponadto zgodnie z wnioskiem Komisji dotyczącym rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)[55] jednostka centralna ETIAS Europejskiej Agencji Straży Granicznej i Przybrzeżnej dokona weryfikacji w SIS za pomocą ETIAS, aby przeprowadzić ocenę wniosków dotyczących zezwolenia na podróż, które wymagają m.in. ustalenia, czy w SIS istnieje wpis dotyczący danego obywatela państwa trzeciego ubiegającego się o

[54] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624 z dnia 14 września 2016 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej oraz zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 i uchylające rozporządzenie (WE) nr 863/2007 Parlamentu Europejskiego i Rady, rozporządzenie Rady (WE) nr 2007/2004 i decyzję Rady 2005/267/WE (Dz.U. L 251 z 16.9.2016, s. 1).

[55] COM(2016) 731 final.

zezwolenie na podróż. W tym celu jednostka centralna ETIAS w ramach Europejskiej Agencji Straży Granicznej i Przybrzeżnej również powinna mieć dostęp do SIS w zakresie niezbędnym do wykonywania jej zadań, a mianowicie do wszystkich kategorii wpisów dotyczących obywateli państw trzecich, w odniesieniu do których dokonano wpisu do celów wjazdu i pobytu oraz którzy objęci są środkiem ograniczającym mającym na celu uniemożliwienie wjazdu lub przejazdu przez państwa członkowskie.

(38) Z uwagi na ich charakter techniczny, poziom szczegółowości i potrzebę regularnej aktualizacji, niektóre aspekty SIS nie mogą zostać wyczerpująco ujęte w przepisach niniejszego rozporządzenia. Dotyczy to np. technicznych zasad wprowadzania danych, aktualizacji, usuwania i wyszukiwania danych, jakości danych i zasad wyszukiwania dotyczących identyfikatorów biometrycznych, zasad dotyczących zgodności i kolejności wpisów, dodawania zastrzeżeń, odsyłaczy do innych wpisów, ustalania terminu wygaśnięcia wpisów w ramach maksymalnego okresu oraz wymiany informacji uzupełniających. W związku z tym uprawnienia wykonawcze w zakresie tych aspektów powinny zostać przyznane Komisji. Techniczne zasady dotyczące wyszukiwania wpisów powinny uwzględniać sprawne działanie aplikacji krajowych.

(39) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011[56]. Procedury przyjmowania środków wykonawczych na mocy niniejszego rozporządzenia i rozporządzenia (UE) 2018/xxx (współpraca policyjna i współpraca wymiarów sprawiedliwości w sprawach karnych) powinny być takie same.

(40) W celu zapewnienia przejrzystości Agencja powinna sporządzać co dwa lata sprawozdanie na temat technicznych aspektów funkcjonowania centralnego SIS i infrastruktury łączności, w tym kwestii ich ochrony oraz wymiany informacji uzupełniających. Komisja powinna dokonywać ogólnej oceny co cztery lata.

(41) W związku z tym, że cele niniejszego rozporządzenia, czyli ustanowienie wspólnego systemu informacji i przyjęcie dotyczących go uregulowań, a także wymiana powiązanych informacji uzupełniających, nie mogą ze względu na swój charakter zostać osiągnięte w wystarczający sposób na szczeblu państw członkowskich, natomiast mogą być lepiej osiągnięte na szczeblu Unii, Unia może podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności, określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(42) Niniejsze rozporządzenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej. W szczególności niniejsze rozporządzenie ma na celu zapewnienie bezpiecznego otoczenia dla wszystkich osób przebywających na terytorium Unii Europejskiej oraz ochronę nielegalnych migrantów przed wykorzystywaniem i handlem ludźmi poprzez umożliwienie ich identyfikacji, przy pełnym poszanowaniu ochrony danych osobowych.

---

[56] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

(43) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczy w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje. Ponieważ niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, zgodnie z art. 4 tego protokołu Dania podejmuje w terminie sześciu miesięcy po przyjęciu przez Radę niniejszego rozporządzenia decyzję, czy dokona jego transpozycji do swego prawa krajowego.

(44) Niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, które nie mają zastosowania do Zjednoczonego Królestwa zgodnie z decyzją Rady 2000/365/WE[57]. Zjednoczone Królestwo nie uczestniczy zatem w przyjęciu niniejszego rozporządzenia, nie jest nim związane ani nie podlega jego stosowaniu.

(45) Niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, które nie mają zastosowania do Irlandii zgodnie z decyzją Rady 2002/192/WE[58]. Irlandia nie uczestniczy zatem w przyjęciu niniejszego rozporządzenia, nie jest nim związana ani go nie stosuje.

(46) W odniesieniu do Islandii i Norwegii niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen – w rozumieniu układu zawartego przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącego włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[59] – które należą do dziedziny, o której mowa w art. 1 lit. G decyzji Rady 1999/437/WE[60] w sprawie niektórych warunków stosowania tego układu.

(47) W odniesieniu do Szwajcarii niniejsze rozporządzenie stanowi rozwinięcie postanowień dorobku Schengen w rozumieniu Umowy podpisanej między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, objętych obszarem, o którym mowa w art. 1 lit. G decyzji 1999/437/WE w związku z art. 4 ust. 1 decyzji Rady 2004/849/WE[61] oraz 2004/860/WE[62].

(48) W odniesieniu do Liechtensteinu niniejsza decyzja stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu o przystąpieniu Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[63], które wchodzą w

---

57 Dz.U. L 131 z 1.6.2000, s. 43.

58 Dz.U. L 64 z 7.3.2002, s. 20.

59 Dz.U. L 176 z 10.7.1999, s. 36.

60 Dz.U. L 176 z 10.7.1999, s. 31.

61 Decyzja Rady 2004/849/WE z dnia 25 października 2004 r. w sprawie podpisania w imieniu Unii Europejskiej oraz tymczasowego stosowania niektórych postanowień Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia tego państwa we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen (Dz.U. L 368 z 15.12.2004, s. 26).

62 Decyzja Rady 2004/860/WE z dnia 25 października 2004 r. w sprawie podpisania w imieniu Wspólnoty Europejskiej oraz tymczasowego stosowania niektórych postanowień Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen (Dz.U. L 370 z 17.12.2004, s. 78).

63 Dz.U. L 160 z 18.6.2011, s. 21.

zakres obszaru, o którym mowa w art. 1 lit. G decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2011/349/UE[64] i art. 3 decyzji Rady 2011/350/UE[65].

(49) W odniesieniu do Bułgarii i Rumunii niniejsze rozporządzenie stanowi akt oparty na dorobku Schengen lub w inny sposób z nim związany w rozumieniu art. 4 ust. 2 Aktu przystąpienia z 2005 r. i należy je czytać w związku z decyzją Rady 2010/365/UE w sprawie stosowania w Republice Bułgarii i w Rumunii przepisów dorobku Schengen związanych z systemem informacyjnym Schengen[66].

(50) W odniesieniu do Cypru i Chorwacji niniejsze rozporządzenie stanowi akt oparty na dorobku Schengen lub w inny sposób z nim związany w rozumieniu odpowiednio art. 3 ust. 2 Aktu przystąpienia z 2003 r. oraz art. 4 ust. 2 Aktu przystąpienia z 2011 r.

(51) Przewidywane w niniejszym rozporządzeniu koszty modernizacji krajowych systemów SIS oraz wprowadzenia nowych funkcji są niższe niż środki pozostałe w linii budżetowej przeznaczonej na inicjatywę na rzecz inteligentnych granic w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 515/2014[67]. W związku z powyższym w niniejszym rozporządzaniu należy ponownie przydzielić kwotę przypisaną na rozwijanie systemów IT wspomagających zarządzanie przepływami migracyjnymi przez granice zewnętrzne zgodnie z art. 5 ust. 5 lit. b) rozporządzenia (UE) nr 515/2014.

(52) Należy zatem uchylić rozporządzenie (WE) nr 1987/2006.

(53) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu [...] r.,

---

64 Decyzja Rady 2011/349/UE z dnia 7 marca 2011 r. w sprawie zawarcia w imieniu Unii Europejskiej Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, odnoszącego się w szczególności do współpracy sądowej w sprawach karnych i współpracy policji (Dz.U. L 160 z 18.6.2011, s. 1).

65 Decyzja Rady 2011/350/UE z dnia 7 marca 2011 r. w sprawie zawarcia w imieniu Unii Europejskiej Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, odnoszącego się do zniesienia kontroli na granicach wewnętrznych i do przemieszczania się osób (Dz.U. L 160 z 18.6.2011, s. 19).

66 Dz.U. L 166 z 1.7.2010, s. 17.

67 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 515/2014 z dnia 16 kwietnia 2014 r. ustanawiające, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument na rzecz wsparcia finansowego w zakresie granic zewnętrznych i wiz (Dz.U. L 150 z 20.5.2014, s. 143).

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1
Ogólny cel SIS

Celem SIS jest zapewnienie – przy wykorzystaniu informacji przekazywanych za pośrednictwem tego systemu – wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii, w tym utrzymywanie bezpieczeństwa publicznego oraz porządku publicznego oraz zagwarantowanie bezpieczeństwa na terytorium państw członkowskich, a także stosowanie postanowień części trzeciej tytuł V rozdział 2 Traktatu o funkcjonowaniu Unii Europejskiej odnoszących się do przepływu osób na terytorium państw członkowskich.

Artykuł 2
Zakres zastosowania

1. Niniejsze rozporządzenie określa warunki i procedury dokonywania oraz przetwarzania w SIS wpisów odnoszących się do obywateli państw trzecich, wymiany informacji uzupełniających i danych dodatkowych w celu odmowy wjazdu i pobytu na terytorium państw członkowskich.

2. Ponadto w niniejszym rozporządzeniu ustanawia się przepisy dotyczące struktury technicznej SIS, obowiązków państw członkowskich i Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, ogólnego przetwarzania danych, praw osób zainteresowanych oraz odpowiedzialności.

Artykuł 3
Definicje

1. Do celów niniejszego rozporządzenia stosuje się następujące definicje:

   a) „wpis” oznacza zbiór danych, w tym identyfikatorów biometrycznych, o których mowa w art. 22, wprowadzonych do SIS, umożliwiających właściwym organom zidentyfikowanie osoby w celu podjęcia konkretnego działania;

   b) „informacje uzupełniające” oznaczają informacje, które nie są częścią danych zawartych we wpisach przechowywanych w SIS, ale są związane z wpisami do SIS, i które są wymieniane w następujących okolicznościach:

      1) w celu umożliwienia państwom członkowskim wzajemnej konsultacji lub wzajemnego informowania się podczas dokonywania wpisu;

2) w celu umożliwienia podjęcia odpowiednich działań po uzyskaniu trafienia w systemie;

3) w przypadku niemożności podjęcia wymaganego działania;

4) w przypadku rozwiązywania kwestii jakości danych SIS;

5) w przypadku rozwiązywania kwestii zgodności i kolejności wpisów;

6) w przypadku rozwiązywania kwestii związanych z prawami dostępu;

c) „dane dodatkowe” oznaczają dane związane z wpisami do SIS, które są przechowywane w SIS i które są natychmiast dostępne dla właściwych organów, gdy w wyniku wyszukiwania prowadzonego w systemie znaleziono w nim osobę, której dane w nim umieszczono;

d) „obywatel państwa trzeciego” oznacza każdą osobę, która nie jest obywatelem Unii w rozumieniu art. 20 TFUE, z wyjątkiem osób, które korzystają z prawa swobodnego przemieszczania się równoważnego z prawem obywateli Unii na mocy porozumień pomiędzy Unią lub Unią i jej państwami członkowskimi z jednej a państwami trzecimi z drugiej strony;

e) „dane osobowe” oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoba, której dotyczą dane”);

f) „możliwa do zidentyfikowania osoba fizyczna” to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

g) „przetwarzanie danych osobowych” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

h) „trafienie” w SIS oznacza, że:

1) użytkownik końcowy przeprowadza wyszukiwanie;

2) w wyniku wyszukiwania znaleziono wpis wprowadzony do SIS przez inne państwo członkowskie;

3) dane dotyczące wpisu w SIS pasują do danych wprowadzonych na potrzeby wyszukiwania; oraz

4) w wyniku uzyskania trafienia wystąpiono o podjęcie dalszych działań;

i) „państwo członkowskie dokonujące wpisu” oznacza państwo członkowskie, które dokonało wpisu w SIS;

j) „państwo członkowskie wykonujące wpis” oznacza państwo członkowskie, które podejmuje wymagane działania po uzyskaniu trafienia w systemie;

k) „użytkownicy końcowi” oznaczają właściwe organy, które bezpośrednio przeszukują CS-SIS, N.SIS lub ich kopie techniczne;

l) „powrót” oznacza powrót zdefiniowany w art. 3 pkt 3 dyrektywy 2008/115/WE;

m) „zakaz wjazdu” oznacza zakaz wjazdu zdefiniowany w art. 3 pkt 6 dyrektywy 2008/115/WE;

n) „dane daktyloskopijne” oznaczają dane dotyczące odwzorowań linii papilarnych palców rąk i dłoni, które z powodu ich niepowtarzalności i układu cech szczególnych umożliwiają dokładne i jednoznaczne ustalenie tożsamości danej osoby;

o) „poważne przestępstwo” oznacza przestępstwa wymienione w art. 2 ust. 1 i 2 decyzji ramowej 2002/584/WSiSW z dnia 13 czerwca 2002 r.[68];

p) „przestępstwa terrorystyczne” oznaczają przestępstwa określone zgodnie z prawem krajowym, o których mowa w art. 1–4 decyzji ramowej 2002/475/WSiSW z dnia 13 czerwca 2002 r.[69].

Artykuł 4
Struktura techniczna i sposoby korzystania z SIS

1. SIS składa się z:

a) systemu centralnego („centralny SIS”) składającego się z następujących elementów:

– funkcji wsparcia technicznego („CS-SIS”) zawierającej bazę danych („baza danych SIS”);

– jednorodnego interfejsu krajowego (NI-SIS);

b) systemu krajowego (N.SIS) w każdym państwie członkowskim, składającego się z krajowych systemów danych, które łączą się z centralnym SIS. N-SIS zawiera plik danych („kopia krajowa”) zawierający pełną lub częściową kopię bazy danych SIS oraz kopię zapasową N.SIS. Aby zapewnić użytkownikom

[68] Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. L 190 z 18.7.2002, s. 1).

[69] Decyzja ramowa Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. L 164 z 22.6.2002, s. 3).

końcowym nieprzerwany dostęp do systemu, istnieje możliwość jednoczesnego korzystania z N.SIS oraz jego kopii zapasowej;

c) infrastruktury łączności pomiędzy CS-SIS a NI-SIS („infrastruktura łączności"), dzięki której dane SIS mogą być przekazywane przez przeznaczoną do tego zaszyfrowaną sieć wirtualną i wymieniane między biurami SIRENE, o których mowa w art. 7 ust. 2.

2. Dane w SIS wpisuje się, aktualizuje, usuwa i wyszukuje za pośrednictwem poszczególnych N.SIS. Częściowa lub pełna kopia krajowa jest dostępna w celu prowadzenia automatycznego wyszukiwania na terytorium każdego państwa członkowskiego, które korzysta z takiej kopii. Częściowa kopia krajowa zawiera co najmniej dane wymienione w art. 20 ust. 2 lit. a)–v) niniejszego rozporządzenia. Przeszukiwanie plików danych zawartych w N.SIS innych państw członkowskich nie jest możliwe.

3. CS-SIS wykonuje funkcje nadzorcze i administracyjne i posiada rezerwowy CS-SIS, zdolny do zapewnienia wszystkich funkcji głównego CS-SIS w przypadku jego awarii. CS-SIS i rezerwowy CS-SIS znajdują się w dwóch lokalizacjach technicznych Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości ustanowionej na mocy rozporządzenia (UE) nr 1077/2011[70] („Agencja"). CS-SIS lub rezerwowy CS-SIS mogą zawierać dodatkową kopię bazy danych SIS i można jednocześnie przeprowadzać na nich aktywne operacje, pod warunkiem że każdy z tych systemów jest w stanie przetworzyć wszystkie transakcje związane z wpisami do SIS.

4. CS-SIS zapewnia usługi konieczne do wprowadzania i przetwarzania danych SIS, w tym do prowadzenia wyszukiwań w bazie danych SIS. CS-SIS zapewnia:

a) aktualizację kopii krajowych w trybie online;

b) synchronizację i spójność kopii krajowych z bazą danych SIS;

c) czynności związane z inicjalizacją i odtwarzaniem kopii krajowych;

d) niezakłóconą dostępność.

Artykuł 5
Koszty

1. Koszty eksploatacji, utrzymania i dalszego rozwoju centralnego SIS oraz infrastruktury łączności są pokrywane z budżetu ogólnego Unii Europejskiej.

2. Koszty te obejmują także koszty prac przeprowadzanych w odniesieniu do CS-SIS, pozwalające zapewniać usługi, o których mowa w art. 4 ust. 4.

[70] Ustanowionej rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. ustanawiającym Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz.U. L 286 z 1.11.2011, s. 1).

3. Koszty budowy, eksploatacji, utrzymania i dalszego rozwoju każdego N.SIS ponosi dane państwo członkowskie.

ROZDZIAŁ II

OBOWIĄZKI PAŃSTW CZŁONKOWSKICH

Artykuł 6
Systemy krajowe

Każde państwo członkowskie odpowiada za budowę, eksploatację, utrzymanie i dalszy rozwój własnego N.SIS oraz za przyłączenie swojego N.SIS do NI-SIS.

Każde państwo członkowskie odpowiada za zapewnienie ciągłej eksploatacji N.SIS, jego połączenia z NI-SIS oraz niezakłóconej dostępności danych z SIS dla użytkowników końcowych.

Artykuł 7
Urząd N.SIS i biuro SIRENE

1. Każde państwo członkowskie wyznacza organ (urząd N.SIS), który na szczeblu centralnym odpowiada za N.SIS tego państwa.

   Organ ten odpowiada za sprawne działanie i bezpieczeństwo N.SIS, zapewnia właściwym organom dostęp do SIS i stosuje odpowiednie środki, aby zapewnić przestrzeganie przepisów niniejszego rozporządzenia. Odpowiada on za zapewnienie, aby wszystkie funkcje SIS były właściwie udostępniane użytkownikom końcowym.

   Każde państwo członkowskie przekazuje swoje wpisy za pośrednictwem urzędu N.SIS.

2. Każde państwo członkowskie wyznacza organ (biuro SIRENE), który zapewnia wymianę i dostępność wszelkich informacji uzupełniających, o których mowa w art. 8, zgodnie z wytycznymi zawartymi w podręczniku SIRENE.

   Powyższe biura koordynują również weryfikację jakości informacji wprowadzanych do SIS. Aby realizować te cele, biura SIRENE posiadają dostęp do danych przetwarzanych w SIS.

3. Państwa członkowskie informują Agencję o swoim urzędzie N.SIS II i biurze SIRENE. Agencja publikuje wykaz tych urzędów i biur wraz z wykazem, o którym mowa w art. 36 ust. 8.

Artykuł 8
Wymiana informacji uzupełniających

1. Informacje uzupełniające są wymieniane zgodnie z wytycznymi zawartymi w podręczniku SIRENE za pośrednictwem infrastruktury łączności. Państwa członkowskie zapewniają niezbędne zasoby techniczne i ludzkie w celu zagwarantowania ciągłej dostępności i wymiany informacji uzupełniających. W przypadku gdy infrastruktura łączności jest niedostępna, państwa członkowskie mogą wykorzystywać inne odpowiednio zabezpieczone środki techniczne do wymiany informacji uzupełniających.

2. Informacje uzupełniające są wykorzystywane wyłącznie do celu, w jakim zostały przekazane zgodnie z art. 43, chyba że uzyskana zostanie uprzednia zgoda państwa członkowskiego dokonującego wpisu.

3. Biura SIRENE realizują swoje zadanie w sposób szybki i skuteczny, w szczególności udzielając jak najszybszej odpowiedzi na wniosek, lecz nie później niż 12 godzin od jego otrzymania.

4. Szczegółowe zasady wymiany informacji uzupełniających przyjmuje się w drodze środków wykonawczych zgodnie z procedurą sprawdzającą określoną w art. 55 ust. 2 w formie „podręcznika SIRENE".

Artykuł 9
Zgodność pod względem technicznym i funkcjonalnym

1. Tworząc własny N.SIS, każde państwo członkowskie przestrzega wspólnych norm, protokołów i procedur technicznych ustalonych, by zapewnić kompatybilność własnych N.SIS z CS-SIS na potrzeby szybkiego i sprawnego przesyłu danych. Wspomniane wspólne normy, protokoły i procedury techniczne określa się i opracowuje w drodze środków wykonawczych zgodnie z procedurą sprawdzającą określoną w art. 55 ust. 2.

2. Korzystając z usług zapewnianych przez CS-SIS, państwa członkowskie zapewniają, by dane przechowywane w kopii krajowej były dzięki automatycznym aktualizacjom, o których mowa w art. 4 ust. 4, identyczne i spójne względem danych w bazie danych SIS oraz by wyszukiwanie kopii krajowej prowadziło do takich samych wyników, jak wyszukiwanie bazy danych SIS. Użytkownicy końcowi otrzymują dane potrzebne do wykonania ich zadań, w szczególności wszystkie dane potrzebne do identyfikacji osoby, której dane dotyczą, oraz do podjęcia odpowiednich działań.

Artykuł 10
Bezpieczeństwo – państwa członkowskie

1. W odniesieniu do N.SIS każde państwo członkowskie przyjmuje niezbędne środki, uwzględniając plan bezpieczeństwa, plan ciągłości działania i plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, aby:

a) zapewnić fizyczną ochronę danych, w tym poprzez sporządzenie planów awaryjnych służących ochronie infrastruktury krytycznej;

b) zapobiec dostępowi osób nieuprawnionych do infrastruktury przetwarzania danych, wykorzystywanej do przetwarzania danych osobowych (kontrola dostępu do infrastruktury);

c) zapobiec nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);

d) zapobiec nieuprawnionemu wprowadzaniu danych i nieuprawnionemu wglądowi do przechowywanych danych osobowych oraz ich zmienianiu i usuwaniu (kontrola przechowywania);

e) zapobiec wykorzystywaniu systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, korzystające ze sprzętu do przekazywania danych (kontrola użytkowników);

f) zapewnić, by osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania danych miały dostęp wyłącznie do danych objętych posiadanym przez siebie upoważnieniem, za pomocą osobistych i niepowtarzalnych identyfikatorów użytkownika oraz poufnego trybu dostępu (kontrola dostępu do danych);

g) zapewnić, by wszystkie organy mające prawo dostępu do SIS lub do infrastruktury przetwarzania danych stworzyły profile z opisem funkcji i zadań osób, które są uprawnione do dostępu do danych oraz do ich wprowadzania, aktualizowania, usuwania i wyszukiwania, oraz by profile te były niezwłocznie udostępniane krajowym organom nadzorczym, o których mowa w art. 50 ust. 1, na ich wniosek (profile personelu);

h) zapewnić możliwość weryfikacji i stwierdzania, jakim organom można przekazywać dane osobowe za pośrednictwem sprzętu do przekazywania danych (kontrola przekazywania danych);

i) zapewnić następnie możliwość późniejszej weryfikacji i stwierdzenia, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania danych oraz kiedy, przez kogo i w jakim celu dane te zostały wprowadzone (kontrola wprowadzania danych);

j) zapobiec nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas transferu danych osobowych lub podczas przemieszczania nośników danych, w szczególności poprzez zastosowanie odpowiednich technik szyfrowania (kontrola transportu);

k) kontrolować skuteczność środków bezpieczeństwa, o których mowa w niniejszym ustępie, oraz podejmować konieczne działania organizacyjne dotyczące kontroli wewnętrznej (autokontrola).

2. Państwa członkowskie podejmują środki równoważne środkom, o których mowa w ust. 1, w odniesieniu do bezpieczeństwa przetwarzana i wymiany informacji uzupełniających, w tym zabezpieczenia terenu biura SIRENE.

3. Państwa członkowskie podejmują środki równoważne środkom, o których mowa w ust. 1, w odniesieniu do bezpieczeństwa przetwarzania danych SIS przez organy, o których mowa w art. 29.

Artykuł 11
Poufność – państwa członkowskie

Każde państwo członkowskie stosuje własne przepisy dotyczące tajemnicy zawodowej lub inne równoważne wymogi poufności wobec wszystkich osób i podmiotów, które muszą operować danymi SIS i informacjami uzupełniającymi, zgodnie z jego prawem krajowym. Zobowiązanie to obowiązuje także po zakończeniu pełnienia urzędu lub ustaniu zatrudnienia oraz po zakończeniu działalności przez dane podmioty.

Artykuł 12
Prowadzenie rejestrów na szczeblu krajowym

1. Państwa członkowskie zapewniają rejestrowanie w N.SIS wszystkich przypadków, w których uzyskano dostęp do CS-SIS lub dokonano wymiany danych osobowych z CS-SIS – w celu kontrolowania, czy dane wyszukiwanie jest dopuszczalne, monitorowania dopuszczalności przetwarzania danych, w celu autokontroli oraz zapewnienia prawidłowego działania N.SIS, a także integralności i bezpieczeństwa danych.

2. Rejestry zawierają w szczególności historię wpisu, datę i godzinę przetworzenia danych, rodzaj danych wykorzystanych do wyszukiwania, odniesienie do rodzaju przekazanych danych oraz nazwę właściwego organu i nazwisko osoby odpowiedzialnej za przetwarzanie danych.

3. Jeżeli wyszukiwanie przeprowadza się z wykorzystaniem danych daktyloskopijnych lub obrazu twarzy zgodnie z art. 22, rejestry zawierają w szczególności rodzaj danych wykorzystanych do wyszukiwania, odniesienie do rodzaju przekazanych danych oraz nazwę właściwego organu i nazwisko osoby odpowiedzialnej za przetwarzanie danych.

4. Rejestry mogą być wykorzystywane wyłącznie do celów, o których mowa w ust. 1, i są usuwane najwcześniej po upływie jednego roku, a najpóźniej po upływie trzech lat od daty ich utworzenia.

5. Rejestry mogą być przechowywane dłużej, jeśli są potrzebne dla celów procedur monitorowania, które już się rozpoczęły.

6. Właściwe organy krajowe odpowiedzialne za kontrolowanie, czy dane wyszukiwanie jest dopuszczalne, monitorowanie dopuszczalności przetwarzania danych, autokontrolę i zapewnianie należytego działania N.SIS, integralności danych i bezpieczeństwa, muszą w granicach swoich uprawnień i na żądanie mieć dostęp do tych rejestrów do celów wykonywania swoich zadań.

Artykuł 13
Autokontrola

Państwa członkowskie zapewniają, aby każdy organ posiadający prawo do dostępu do SIS podejmował konieczne działania w celu zapewnienia zgodności z przepisami niniejszego rozporządzenia i, w razie potrzeby, współpracował z krajowym organem nadzorczym.

Artykuł 14
Szkolenie personelu

Przed otrzymaniem upoważnienia do przetwarzania danych przechowywanych w SIS i okresowo po przyznaniu dostępu do danych SIS personel organów mających prawo dostępu do SIS przechodzi odpowiednie przeszkolenie w zakresie zasad bezpieczeństwa, ochrony danych oraz procedur z zakresu przetwarzania danych określonych w podręczniku SIRENE. Członkowie personelu zostają pouczeni o wszelkich związanych z tym przestępstwach i sankcjach.

ROZDZIAŁ III

OBOWIĄZKI AGENCJI

Artykuł 15
Zarządzanie operacyjne

1. Agencja odpowiada za zarządzanie operacyjne centralnym SIS. Korzystając z analizy kosztów i korzyści, Agencja – we współpracy z państwami członkowskimi – zapewnia, by w centralnym SIS stosowane były zawsze najlepsze dostępne technologie.

2. Agencja odpowiedzialna jest również za następujące zadania związane z infrastrukturą łączności:

   a) nadzór;

   b) bezpieczeństwo;

   c) koordynację stosunków między państwami członkowskimi a dostawcą usług.

3. Komisja jest odpowiedzialna za realizację wszystkich pozostałych zadań związanych z infrastrukturą łączności, w szczególności za:

   a) zadania związane z wykonywaniem budżetu;

   b) zakupy i odnawianie;

   c) kwestie dotyczące umów.

4. Agencja jest też odpowiedzialna za następujące zadania związane z biurami SIRENE i komunikacją między biurami SIRENE:

a) koordynację testów i zarządzanie nimi;

b) utrzymanie i aktualizowanie specyfikacji technicznych dotyczących wymiany informacji uzupełniających między biurami SIRENE a infrastrukturą łączności oraz zarządzanie wpływem zmian technicznych, gdy dotyczy on zarówno SIS, jak i wymiany informacji uzupełniających między biurami SIRENE.

5. Agencja opracowuje i utrzymuje mechanizm i procedury do celów przeprowadzania kontroli jakości danych CS-SIS i regularnie przekazuje sprawozdania państwom członkowskim. Agencja regularnie przekazuje Komisji sprawozdania, w których uwzględnia wszystkie napotkane problemy i państwa członkowskie, których one dotyczą. Mechanizm, procedury i interpretację zgodności jakości danych określa się i opracowuje w drodze środków wykonawczych zgodnie z procedurą sprawdzającą określoną w art. 55 ust. 2.

6. Zarządzanie operacyjne centralnym SIS obejmuje wszystkie zadania niezbędne do tego, by centralny SIS działał zgodnie z niniejszym rozporządzeniem przez 24 godziny na dobę, 7 dni w tygodniu – w szczególności prace konserwacyjne oraz udoskonalenia technologiczne, jakich wymaga sprawne działanie systemu. Zadania te obejmują również działania z zakresu testowania, zapewniające funkcjonowanie centralnego SIS i systemów krajowych zgodnie z wymogami technicznymi i funkcjonalnymi określonymi w art. 9 niniejszego rozporządzenia.

Artykuł 16
Bezpieczeństwo

1. Agencja przyjmuje niezbędne środki, obejmujące plan bezpieczeństwa, plan ciągłości działania i plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, dotyczące centralnego SIS i infrastruktury łączności, aby:

a) zapewnić fizyczną ochronę danych, w tym poprzez sporządzenie planów awaryjnych służących ochronie infrastruktury krytycznej;

b) zapobiec dostępowi osób nieuprawnionych do infrastruktury przetwarzania danych, wykorzystywanej do przetwarzania danych osobowych (kontrola dostępu do infrastruktury);

c) zapobiec nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);

d) zapobiec nieuprawnionemu wprowadzaniu danych i nieuprawnionemu wglądowi do przechowywanych danych osobowych oraz ich zmienianiu i usuwaniu (kontrola przechowywania);

e) zapobiec wykorzystywaniu systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, korzystające ze sprzętu do przekazywania danych (kontrola użytkowników);

f) zapewnić, by osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania danych miały dostęp wyłącznie do danych objętych posiadanym przez siebie upoważnieniem, za pomocą osobistych i niepowtarzalnych

identyfikatorów użytkownika oraz poufnego trybu dostępu (kontrola dostępu do danych);

g) stworzyć profile z opisem funkcji i zadań osób, które są uprawnione do dostępu do danych lub do infrastruktury przetwarzania danych, i udostępnić te profile bezzwłocznie Europejskiemu Inspektorowi Ochrony Danych, o którym mowa w art. 51, na jego wniosek (profile personelu);

h) zapewnić możliwość weryfikacji i stwierdzania, jakim organom można przekazywać dane osobowe za pośrednictwem sprzętu do przekazywania danych (kontrola przekazywania danych);

i) zapewnić następnie możliwość weryfikacji i stwierdzania, które dane osobowe zostały wprowadzone do zautomatyzowanych systemów przetwarzania danych oraz kiedy i przez kogo zostały one wprowadzone (kontrola wprowadzania danych);

j) zapobiec nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas transferu danych osobowych lub podczas przemieszczania nośników danych, w szczególności poprzez zastosowanie odpowiednich technik szyfrowania (kontrola transportu);

k) kontrolować skuteczność środków bezpieczeństwa, o których mowa w niniejszym ustępie, i podejmować konieczne działania organizacyjne dotyczące kontroli wewnętrznej, tak by spełnić wymogi niniejszego rozporządzenia (autokontrola).

2. W odniesieniu do bezpieczeństwa przetwarzania i wymiany informacji uzupełniających za pomocą infrastruktury łączności Agencja podejmuje środki bezpieczeństwa równoważne środkom, o których mowa w ust. 1.

Artykuł 17
Poufność – Agencja

1. Bez uszczerbku dla art. 17 Regulaminu pracowniczego urzędników Unii Europejskiej i warunków zatrudnienia innych pracowników Unii Europejskiej Agencja stosuje odpowiednie zasady tajemnicy zawodowej lub inne równoważne wymogi poufności wobec wszystkich swoich pracowników, którzy muszą operować danymi SIS, na zasadach porównywalnych z zasadami, o których mowa w art. 11 niniejszego rozporządzenia. Zobowiązanie to obowiązuje również po zakończeniu pełnienia urzędu lub ustaniu zatrudnienia lub po zakończeniu ich działalności.

2. W odniesieniu do poufności wymiany informacji uzupełniających za pomocą infrastruktury łączności Agencja podejmuje środki zapewniające poufność równoważne środkom, o których mowa w ust. 1.

Artykuł 18
Prowadzenie rejestrów na szczeblu centralnym

1. Agencja zapewnia rejestrowanie wszystkich przypadków, w których uzyskano dostęp do danych osobowych w CS-SIS lub dokonano wymiany takich danych, do celów, o których mowa w art. 12 ust. 1.

2. Rejestry zawierają w szczególności historię wpisów, datę i godzinę przekazania danych, rodzaj danych wykorzystanych do wyszukiwania, odniesienie do rodzaju przekazanych danych oraz nazwę właściwego organu odpowiedzialnego za przetwarzanie danych.

3. Jeżeli wyszukiwanie przeprowadza się z wykorzystaniem danych daktyloskopijnych lub obrazu twarzy zgodnie z art. 22 i 28, rejestry zawierają w szczególności rodzaj danych wykorzystanych do wyszukiwania, odniesienie do rodzaju danych przekazanych oraz nazwę właściwego organu i nazwisko osoby odpowiedzialnej za przetwarzanie danych.

4. Rejestry mogą być wykorzystywane wyłącznie do celów wskazanych w ust. 1 i są usuwane najwcześniej po upływie jednego roku, a najpóźniej po upływie trzech lat od daty ich sporządzenia. Rejestry obejmujące historię wpisów są usuwane po upływie okresu od jednego roku do trzech lat od daty usunięcia wpisów.

5. Rejestry mogą być przechowywane dłużej, jeśli są potrzebne dla celów procedur monitorowania, które już się rozpoczęły.

6. Właściwe organy odpowiedzialne za kontrolowanie, czy dane wyszukiwanie jest dopuszczalne, monitorowanie dopuszczalności przetwarzania danych, autokontrolę i zapewnianie należytego działania CS-SIS, integralności i bezpieczeństwa danych, muszą – w granicach swoich uprawnień – na żądanie mieć dostęp do tych rejestrów, do celów wykonywania swoich zadań.

ROZDZIAŁ IV

INFORMOWANIE OPINII PUBLICZNEJ

Artykuł 19
Kampanie informacyjne dotyczące SIS

Komisja – we współpracy z krajowymi organami nadzoru i Europejskim Inspektorem Ochrony Danych – regularnie organizuje kampanie informacyjne, w ramach których udziela opinii publicznej informacji na temat celów SIS, danych gromadzonych w tym systemie, organów mających dostęp do SIS oraz praw przysługujących poszczególnym osobom, których dane dotyczą. Państwa członkowskie, we współpracy z własnymi krajowymi organami nadzorczymi, opracowują i wprowadzają w życie konieczne strategie działań służące ogólnemu informowaniu społeczeństwa o SIS.

ROZDZIAŁ V

WPISY DOTYCZĄCE OBYWATELI PAŃSTW TRZECICH DOKONANE DO CELÓW ODMOWY POZWOLENIA NA WJAZD I POBYT

Artykuł 20
Kategorie danych

1. Bez uszczerbku dla art. 8 ust. 1 ani dla przepisów niniejszego rozporządzenia dotyczących przechowywania danych dodatkowych, SIS zawiera wyłącznie te kategorie danych dostarczanych przez każde z państw członkowskich, jakich wymagają cele określone w art. 24.

2. Informacje na temat osób, w odniesieniu do których został dokonany wpis, obejmują następujące dane:

   a) nazwisko (nazwiska);

   b) imiona;

   c) nazwisko(-a) rodowe;

   d) poprzednio używane imiona i nazwiska oraz wszelkie aliasy;

   e) wszelkie szczególne, obiektywne cechy fizyczne niepodlegające zmianom;

   f) miejsce urodzenia;

   g) datę urodzenia;

   h) płeć;

   i) obywatelstwo/obywatelstwa;

   j) informację, czy dana osoba jest uzbrojona, agresywna, czy jest uciekinierem lub czy uczestniczy w działaniu, o którym mowa w art. 1, 2, 3 i 4 decyzji ramowej Rady 2002/475/WSiSW w sprawie zwalczania terroryzmu;

   k) powód wpisu;

   l) organ dokonujący wpisu;

   m) odesłanie do decyzji będącej powodem wpisu;

   n) działania, jakie należy podjąć;

   o) odsyłacz lub odsyłacze do innych wpisów dokonanych w SIS zgodnie z art. 38;

p) informację, czy dana osoba jest członkiem rodziny obywatela UE lub innej osoby, która korzysta z prawa swobodnego przemieszczania się, o której mowa w art. 25;

q) informację, czy podstawą decyzji o odmowie wjazdu jest:

– wcześniejszy wyrok skazujący, o którym mowa w art. 24 ust. 2 lit. a);

– poważne zagrożenie bezpieczeństwa, o którym mowa w art. 24 ust. 2 lit. b);

– zakaz wjazdu, o którym mowa w art. 24 ust. 3; lub

– środek ograniczający, o którym mowa w art. 27;

r) rodzaj przestępstwa (w przypadku wpisów dokonanych zgodnie z art. 24 ust. 2 niniejszego rozporządzenia);

s) kategorię dokumentu identyfikacyjnego danej osoby;

t) państwo wydania dokumentu identyfikacyjnego danej osoby;

u) numer lub numery dokumentu identyfikacyjnego danej osoby;

v) datę wydania dokumentu identyfikacyjnego danej osoby;

w) fotografie i wizerunki twarzy;

x) dane daktyloskopijne;

y) kolorową kopię dokumentu identyfikacyjnego.

3. Techniczne zasady wpisywania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 2, określa się i opracowuje w drodze środków wykonawczych zgodnie z procedurą sprawdzającą, o której mowa w art. 55 ust. 2.

4. Techniczne zasady wyszukiwania danych, o których mowa w ust. 2, określa się i opracowuje zgodnie z procedurą sprawdzającą, o której mowa w art. 55 ust. 2. Wspomniane techniczne zasady są podobne do zasad wyszukiwania w CS-SIS, w kopiach krajowych i technicznych, o których mowa w art. 36, a ich podstawę stanowią wspólne normy określone i opracowane w drodze środków wykonawczych zgodnie z procedurą sprawdzającą, o której mowa w art. 55 ust. 2.

Artykuł 21
Proporcjonalność

1. Przed dokonaniem wpisu i z chwilą wydłużenia okresu ważności wpisu państwa członkowskie decydują, czy dany przypadek jest na tyle stosowny, odpowiedni i ważny, by uzasadnione było wprowadzenie tego wpisu do SIS.

2. Stosując art. 24 ust. 2, państwa członkowskie dokonują takiego wpisu we wszystkich okolicznościach w odniesieniu do obywateli państw trzecich, jeżeli przestępstwo

wchodzi w zakres art. 1–4 decyzji ramowej Rady 2002/475/WSiSW w sprawie zwalczania terroryzmu[71].

Artykuł 22
Zasady szczegółowe dotyczące wprowadzania fotografii, obrazów twarzy i danych daktyloskopijnych

1. Dane, o których mowa w art. 20 ust. 2 lit. w) i x), wprowadzane są do SIS dopiero po przeprowadzeniu kontroli jakości stwierdzającej, czy spełniają minimalny standard jakości danych.

2. Należy ustanowić normy jakości w odniesieniu do przechowywania danych, o których mowa w ust. 1. Specyfikację tych norm określa się w drodze środków wykonawczych i aktualizuje zgodnie z procedurą sprawdzającą określoną w art. 55 ust. 2.

Artykuł 23
Wymóg warunkujący dokonanie wpisu

1. Wpisu nie wolno dokonywać, jeśli brak jest danych, o których mowa w art. 20 ust. 2 lit. a), g), k), m), n) oraz q). Jeżeli podstawą wpisu jest decyzja podjęta na mocy art. 24 ust. 2, wprowadza się również dane, o których mowa w art. 20 ust. 2 lit. r).

2. Wprowadzane są również wszystkie pozostałe dane wymienione w art. 20 ust. 2, o ile są dostępne.

Artykuł 24
Warunki dokonywania wpisów dotyczących odmowy pozwolenia na wjazd i pobyt

1. Dane dotyczące obywateli państw trzecich, w odniesieniu do których został dokonany wpis w celu odmowy pozwolenia na wjazd i pobyt, wprowadza się do SIS na podstawie krajowego wpisu wynikającego z decyzji podjętej na podstawie indywidualnej oceny przez właściwe organy administracyjne lub sądowe zgodnie z zasadami proceduralnymi określonymi w prawie krajowym. Postępowanie odwoławcze w sprawie takich decyzji jest prowadzone zgodnie z przepisami krajowymi.

2. Wpisu dokonuje się, jeżeli decyzja, o której mowa w ust. 1, jest uzasadniona zagrożeniem dla porządku publicznego, bezpieczeństwa publicznego lub bezpieczeństwa narodowego, jakie może stwarzać obecność danego obywatela państwa trzeciego na terytorium państwa członkowskiego. Sytuacja taka ma miejsce w szczególności w przypadku:

   a) obywatela państwa trzeciego, który został skazany w państwie członkowskim za przestępstwo zagrożone karą pozbawienia wolności powyżej jednego roku;

[71] Decyzja ramowa Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. L 164 z 22.6.2002, s. 3).

b) obywatela państwa trzeciego, co do którego istnieją uzasadnione powody, by sądzić, że popełnił poważne przestępstwo, lub co do którego istnieją poważne przesłanki, by sądzić, że zamierza on takie przestępstwo popełnić na terytorium państwa członkowskiego.

3. Wpisu dokonuje się, jeżeli decyzja, o której mowa w ust. 1, jest zakazem wjazdu wydanym zgodnie z procedurami zgodnymi z dyrektywą 2008/115/WE. Państwo członkowskie dokonujące wpisu zapewnia, by wpis stawał się skuteczny w SIS w momencie powrotu danego obywatela państwa trzeciego. Potwierdzenie powrotu jest przekazywane państwu członkowskiemu dokonującemu wpisu zgodnie z art. 6 rozporządzenia (UE) 2018/xxx [rozporządzenie w sprawie powrotów].

Artykuł 25
Warunki dokonywania wpisów dotyczących obywateli państw trzecich korzystających z prawa do swobodnego przepływu w obrębie Unii

1. Wpisu dotyczącego obywatela państwa trzeciego korzystającego z prawa do swobodnego przepływu w obrębie Unii w rozumieniu dyrektywy 2004/38/WE Parlamentu Europejskiego i Rady[72] dokonuje się zgodnie ze środkami przyjętymi w celu wdrożenia tej dyrektywy.

2. W przypadku trafienia dotyczącego wpisu dokonanego zgodnie z art. 24 i dotyczącego obywatela państwa trzeciego korzystającego z prawa do swobodnego przepływu w obrębie Unii, państwo członkowskie wykonujące wpis niezwłocznie konsultuje się w drodze wymiany informacji uzupełniających z państwem członkowskim dokonującym wpisu, by bezzwłocznie podjąć decyzję co do wymaganych działań.

Artykuł 26
Procedura konsultacji

1. Jeżeli państwo członkowskie rozważa przyznanie dokumentu pobytowego lub innego zezwolenia na pobyt obywatelowi państwa trzeciego, którego dotyczy wpis dotyczący odmowy wjazdu i pobytu dokonany przez inne państwo członkowskie, najpierw konsultuje się z państwem członkowskim dokonującym wpisu w drodze wymiany informacji uzupełniających i uwzględnia interesy tego państwa członkowskiego. Państwo członkowskie dokonujące wpisu udziela ostatecznej odpowiedzi w terminie siedmiu dni. Wpis dotyczący odmowy wjazdu i pobytu usuwa się, jeżeli państwo członkowskie, które rozważa przyznanie karty pobytu lub innego zezwolenia na pobyt, postanowi je przyznać.

2. Jeżeli państwo członkowskie rozważa dokonanie wpisu dotyczącego odmowy wjazdu i pobytu dotyczącego obywatela państwa trzeciego, który posiada ważny dokument pobytowy lub inne zezwolenie na pobyt wydane przez inne państwo członkowskie, najpierw konsultuje się w drodze wymiany informacji uzupełniających z państwem członkowskim, które wydało zezwolenie, i uwzględnia interesy tego państwa członkowskiego. Państwo członkowskie, które wydało

[72] Dz.U. L 158 z 30.4.2004, s. 77.

zezwolenie, udziela ostatecznej odpowiedzi w terminie siedmiu dni. Jeżeli państwo członkowskie, które wydało zezwolenie, postanawia utrzymać jego ważność, nie dokonuje się wpisu dotyczącego odmowy wjazdu i pobytu.

3. W przypadku trafienia dotyczącego wpisu dotyczącego odmowy wjazdu i pobytu w odniesieniu do obywatela państwa trzeciego, który posiada ważny dokument pobytowy lub inne zezwolenie na pobyt, państwo członkowskie wykonujące wpis niezwłocznie konsultuje się w drodze wymiany informacji uzupełniających odpowiednio z państwem członkowskim, które wydało dokument pobytowy, oraz państwem członkowskim dokonującym wpisu w celu zadecydowania bez zbędnej zwłoki, czy można podjąć działanie. Jeżeli postanowiono utrzymać ważność dokumentu pobytowego, wpis usuwa się.

4. Państwa członkowskie corocznie dostarczają Agencji statystyki dotyczące konsultacji przeprowadzonych zgodnie z ust. 1–3.

Artykuł 27
Warunki dokonywania wpisów dotyczących obywateli państw trzecich, którzy podlegają środkom ograniczającym

1. Wpisy dotyczące obywateli państw trzecich, wobec których to obywateli zostały podjęte środki ograniczające mające na celu uniemożliwienie wjazdu na terytorium państw członkowskich lub przejazdu przez nie, podjęte zgodnie z aktami prawnymi przyjętymi przez Radę, w tym środki służące wykonaniu zakazu podróży wydanego przez Radę Bezpieczeństwa Organizacji Narodów Zjednoczonych, są wprowadzane do SIS w celu odmowy pozwolenia na wjazd i pobyt, o ile spełnione są wymagania dotyczące jakości danych.

2. Państwo członkowskie odpowiedzialne za dokonywanie, aktualizowanie i usuwanie wpisów w imieniu wszystkich państw członkowskich jest wyznaczane w chwili przyjmowania odpowiedniego środka, podejmowanego zgodnie z art. 29 Traktatu o Unii Europejskiej. Procedurę wyznaczenia odpowiedzialnego państwa członkowskiego określa się i opracowuje w drodze środków wykonawczych zgodnie z procedurą sprawdzającą określoną w art. 55 ust. 2.

ROZDZIAŁ VI

PRZESZUKIWANIE ZA POMOCĄ DANYCH BIOMETRYCZNYCH

Artykuł 28
Zasady szczegółowe dotyczące weryfikacji lub wyszukiwania fotografii, obrazów twarzy i danych daktyloskopijnych

1. Fotografie, obrazy twarzy i dane daktyloskopijne uzyskuje się z systemu SIS w celu potwierdzenia tożsamości osoby, która została znaleziona w wyniku wyszukiwania według danych alfanumerycznych przeprowadzonego w SIS.

2. Dane daktyloskopijne można wykorzystać również do zidentyfikowania danej osoby. Dane daktyloskopijne przechowywane w SIS stosuje się do celów identyfikacji wtedy, gdy tożsamości osoby nie można potwierdzić przy zastosowaniu innych środków.

3. Dane daktyloskopijne przechowywane w SIS w związku z wpisami dokonanymi zgodnie z art. 24 można wyszukiwać również przy użyciu kompletnych lub niekompletnych linii papilarnych lub odcisków dłoni znalezionych na miejscu przestępstwa będącego przedmiotem dochodzenia oraz jeżeli z dużym prawdopodobieństwem można stwierdzić, że należą one do sprawcy przestępstwa, pod warunkiem że właściwe organy nie są w stanie określić tożsamości osoby przy użyciu jakiejkolwiek innej krajowej, europejskiej lub międzynarodowej bazy danych.

4. Gdy tylko stanie się to technicznie możliwe oraz przy jednoczesnym zapewnieniu wysokiego stopnia wiarygodności identyfikacji, do identyfikacji można wykorzystać fotografie i wizerunki twarzy. Z identyfikacji opartej na fotografiach lub wizerunkach twarzy korzysta się wyłącznie na legalnych przejściach granicznych, na których wykorzystuje się systemy samoobsługowe i zautomatyzowane systemy kontroli granicznej.

ROZDZIAŁ VII

PRAWO DO DOSTĘPU I PRZECHOWYWANIE WPISÓW

Artykuł 29
Organy uprawnione do dostępu do wpisów

1. Dostęp do danych wprowadzonych do SIS oraz prawo do ich wyszukiwania bezpośrednio lub w kopii danych SIS są zastrzeżone dla organów odpowiedzialnych za ustalanie tożsamości obywateli państw trzecich do celów:

   a) kontroli granicznej zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulującego przepływ osób przez granice (kodeks graniczny Schengen);

   b) kontroli policyjnych i celnych prowadzonych na terytorium danego państwa członkowskiego oraz koordynacji takich kontroli przez wyznaczone organy;

   c) innych czynności z zakresu ścigania przestępstw wykonywanych w celu zapobiegania przestępstwom, wykrywania przestępstw i prowadzenia dochodzeń dotyczących przestępstw w danym państwie członkowskim;

   d) badania warunków i podejmowania decyzji dotyczących wjazdu i pobytu obywateli państwa trzeciego na terytorium państw członkowskich, w tym dotyczących dokumentów pobytowych i wiz długoterminowych oraz powrotu obywateli państw trzecich;

   e) rozpatrywania wniosków wizowych oraz podejmowania decyzji w sprawie tych wniosków, w tym decyzji o unieważnieniu, cofnięciu lub przedłużeniu

wizy, zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 810/2009[73].

2. Dla celów art. 24 ust. 2 i 3 oraz art. 27 prawo dostępu do danych wprowadzonych do SIS oraz prawo do bezpośredniego wyszukiwania takich danych mogą być wykonywane również przez krajowe organy wymiaru sprawiedliwości, w tym odpowiedzialne za wszczynanie postępowań z oskarżenia publicznego na postawie przepisów prawa karnego i prowadzenie dochodzeń sądowych przed wniesieniem aktu oskarżenia, w ramach wykonywania zadań określonych przez prawo krajowe, a także przez organy pełniące wobec nich funkcję koordynującą.

3. Prawo dostępu do danych dotyczących dokumentów odnoszących się do osób wprowadzonych zgodnie z art. 38 ust. 2 lit. j) i k) rozporządzenia (UE) 2018/xxx [współpraca policyjna i współpraca wymiarów sprawiedliwości w sprawach karnych] oraz prawo do wyszukiwania takich danych mogą być wykonywane również przez organy, o którym mowa w ust. 1 lit. d). Dostęp tych organów do danych jest regulowany prawem każdego z państw członkowskich.

4. Organy, o których mowa w niniejszym artykule, są uwzględniane w wykazie, o którym mowa w art. 36 ust. 8.

Artykuł 30
Dostęp Europolu do danych zawartych w SIS

1. W ramach swojego mandatu Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) ma prawo dostępu do danych wprowadzonych do SIS oraz do ich wyszukiwania.

2. Jeżeli podczas wyszukiwania danych Europol stwierdzi istnienie wpisu w SIS, informuje o tym – metodami określonymi w rozporządzenie (UE) 2016/794 – państwo członkowskie dokonujące wpisu.

3. Wykorzystanie informacji uzyskanych w wyniku wyszukiwania danych SIS wymaga zgody danego państwa członkowskiego. Jeżeli to państwo członkowskie pozwoli na wykorzystanie takich informacji, posługiwanie się nimi przez Europol podlega przepisom rozporządzenia (UE) 2016/794. Europol może przekazać takie informacje państwom trzecim i organom trzecim wyłącznie za zgodą danego państwa członkowskiego.

4. Europol może wystąpić o przekazanie przez dane państwo członkowskie dalszych informacji zgodnie z przepisami rozporządzenia (UE) 2016/794.

5. Europol:

   a) bez uszczerbku dla ust. 3, 4 i 6 nie podłącza części SIS ani też nie przenosi danych, które są w tych częściach zawarte i które zostały mu udostępnione, do jakiegokolwiek komputerowego systemu gromadzenia i przetwarzania danych

[73] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiające Wspólnotowy Kodeks Wizowy (kodeks wizowy) (Dz.U. L 243 z 15.9.2009, s. 1).

stosowanego przez Europol lub w tym urzędzie, a także nie pobiera ani nie kopiuje w inny sposób jakichkolwiek części SIS;

b) ogranicza dostęp do danych wprowadzonych do SIS w taki sposób, by korzystali z niego tylko specjalnie uprawnieni pracownicy Europolu;

c) przyjmuje i stosuje środki przewidziane w art. 10 i 11;

d) zapewnia Europejskiemu Inspektorowi Ochrony Danych możliwość sprawdzenia, w jaki sposób Europol korzysta z prawa dostępu do danych wprowadzonych do SIS i ich wyszukiwania.

6. Dane mogą być kopiowane wyłącznie do celów technicznych, pod warunkiem że takie kopiowanie jest niezbędne do przeprowadzenia bezpośredniego wyszukiwania przez należycie uprawnionych pracowników Europolu. Do takich kopii mają zastosowanie przepisy niniejszego rozporządzenia. Kopię techniczną wykorzystuje się wyłącznie do przechowywania danych SIS w trakcie ich wyszukiwania. Po wyszukaniu danych kopia ta jest usuwana. Zastosowania takiego nie należy interpretować jako niezgodnego z prawem pobierania lub kopiowania danych SIS. Europol nie kopiuje do innych systemów Europolu danych zawartych we wpisach lub danych dodatkowych wydanych przez państwa członkowskie ani danych z CS-SIS.

7. Kopie, o których mowa w ust. 6, przekształcane w bazy danych istniejące w trybie offline mogą być przechowywane przez okres nieprzekraczający 48 godzin. Okres ten może zostać przedłużony w sytuacjach awaryjnych do czasu ich ustania. Europol zgłasza przypadki takiego przedłużenia Europejskiemu Inspektorowi Ochrony Danych.

8. Europol może otrzymywać i przetwarzać informacje uzupełniające dotyczące odpowiadających wpisów SIS, pod warunkiem że obowiązują odpowiednie zasady dotyczące przetwarzania danych, o których mowa w ust. 2–7.

9. Do celów weryfikacji zgodnego z prawem przetwarzania danych, autokontroli i zapewniania właściwego bezpieczeństwa danych oraz ich integralności Europol powinien prowadzić rejestry dostępu do danych zawartych w SIS oraz ich wyszukiwania. Prowadzenia takich rejestrów i dokumentacji nie należy interpretować jako niezgodnego z prawem pobierania lub kopiowania jakiejkolwiek części SIS.

Artykuł 31

Dostęp zespołów Europejskiej Straży Granicznej i Przybrzeżnej, zespołów składających się z personelu realizującego zadania w dziedzinie powrotów oraz członków zespołów wspierających zarządzanie migracjami do danych SIS

1. Zgodnie z art. 40 ust. 8 rozporządzenia (UE) 2016/1624 członkowie zespołów Europejskiej Straży Granicznej i Przybrzeżnej lub zespołów składających się z personelu realizującego zadania w dziedzinie powrotów oraz członkowie zespołu wspierającego zarządzanie migracjami mają prawo, w ramach swojego mandatu, do uzyskania dostępu do danych wprowadzanych do SIS oraz do wyszukiwania tego rodzaju danych.

2. Członkowie zespołów Europejskiej Straży Granicznej i Przybrzeżnej lub zespołów składających się z personelu realizującego zadania w dziedzinie powrotów oraz członkowie zespołu wspierającego zarządzanie migracjami uzyskują dostęp do danych wprowadzanych do SIS oraz do wyszukiwania tego rodzaju danych zgodnie z ust. 1, korzystając z interfejsu technicznego ustanowionego i prowadzonego przez Europejską Agencję Straży Granicznej i Przybrzeżnej zgodnie z art. 32 ust. 2.

3. Jeżeli podczas wyszukiwania członek zespołów Europejskiej Straży Granicznej i Przybrzeżnej, zespołów składających się z personelu realizującego zadania w dziedzinie powrotów lub zespołów wspierających zarządzanie migracjami stwierdzi istnienie wpisu w SIS, powiadamia się o tym fakcie państwo członkowskie dokonujące wpisu. Zgodnie z art. 40 rozporządzenia (UE) 2016/1624 członkowie zespołów mogą podejmować działania w odpowiedzi na wpis w SIS jedynie na polecenie i, co do zasady, w obecności funkcjonariuszy straży granicznej lub personelu realizującego zadania w dziedzinie powrotów przyjmującego państwa członkowskiego, w którym działają. Przyjmujące państwo członkowskie może upoważnić członków zespołów do działania w jego imieniu.

4. Każdy przypadek uzyskania dostępu i przeprowadzenia wyszukiwania przez członka zespołów Europejskiej Straży Granicznej i Przybrzeżnej lub zespołów składających się z personelu realizującego zadania w dziedzinie powrotów lub przez członka zespołów wspierających zarządzanie migracjami zostaje zarejestrowany zgodnie z przepisami art. 12; rejestracji podlega również każde wykorzystanie przez nich danych, do których uzyskali dostęp.

5. Dostęp do danych wprowadzonych do SIS jest ograniczony do członków zespołów Europejskiej Straży Granicznej i Przybrzeżnej, zespołów składających się z personelu realizującego zadania w dziedzinie powrotów lub zespołów wspierających zarządzanie migracjami i nie jest on rozszerzany na żadnych innych członków zespołu.

6. Przyjmowane i stosowane są środki mające na celu zapewnienie bezpieczeństwa i poufności przewidziane w art. 10 i 11.

Artykuł 32
Dostęp Europejskiej Agencji Straży Granicznej i Przybrzeżnej do danych SIS

1. Do celów analizy zagrożeń, które mogą wpłynąć na funkcjonowanie lub bezpieczeństwo granic zewnętrznych, Europejska Agencja Straży Granicznej i Przybrzeżnej ma prawo do dostępu do danych wprowadzonych do SIS i ich wyszukiwania zgodnie z art. 24 i 27.

2. Do celów art. 31 ust. 2 i ust. 1 niniejszego artykułu Europejska Agencja Straży Granicznej i Przybrzeżnej ustanawia i prowadzi interfejs techniczny, który umożliwia bezpośrednie połączenie z centralnym SIS.

3. Jeżeli podczas wyszukiwania danych Europejska Agencja Straży Granicznej i Przybrzeżnej stwierdzi istnienie wpisu w SIS, informuje o tym państwo członkowskie dokonujące wpisu.

4. Do celów realizacji zadań przekazanych na mocy rozporządzenia w sprawie ustanowienia europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS) Europejska Agencja Straży Granicznej i Przybrzeżnej ma prawo do dostępu do danych wprowadzonych do SIS zgodnie z art. 24 i 27 oraz do ich weryfikacji.

5. Jeżeli podczas weryfikacji dla celów ust. 2 Europejska Agencja Straży Granicznej i Przybrzeżnej stwierdzi istnienie wpisu w SIS, zastosowanie ma procedura określona w art. 22 rozporządzenia ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS).

6. Przepisy niniejszego artykułu nie mogą być interpretowane jako modyfikacja tych przepisów rozporządzenia (UE) 2016/1624, które dotyczą ochrony danych i odpowiedzialności prawnej za wszelkie nieuprawnione lub nieprawidłowe przetwarzanie takich danych przez Europejską Agencję Straży Granicznej i Przybrzeżnej.

7. Każdy przypadek uzyskania dostępu i przeprowadzenia wyszukiwania przez Europejską Agencję Straży Granicznej i Przybrzeżnej zostaje zarejestrowany zgodnie z przepisami art. 12; rejestracji podlega również każde wykorzystanie danych, do których Europejska Agencja Straży Granicznej i Przybrzeżnej uzyskała dostęp.

8. Z wyjątkiem sytuacji, w których istnieje konieczność wykonania zadań na potrzeby rozporządzenia ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS), żadnych części SIS nie podłącza się do jakiegokolwiek systemu komputerowego służącego do gromadzenia i przetwarzania danych obsługiwanego przez Europejską Agencję Straży Granicznej i Przybrzeżnej lub w jej siedzibie, a danych zawartych w SIS, udostępnianych Europejskiej Agencji Straży Granicznej i Przybrzeżnej, nie przesyła się do jakiegokolwiek takiego systemu. Nie można pobierać żadnych części SIS. Rejestrowania przypadków dostępu i wyszukiwania nie należy interpretować jako pobierania lub kopiowania danych SIS.

9. Przyjmowane i stosowane są środki mające na celu zapewnienie bezpieczeństwa i poufności przewidziane w art. 10 i 11.

Artykuł 33
Zakres dostępu

Użytkownicy końcowi, w tym Europol oraz Europejska Agencja Straży Granicznej i Przybrzeżnej, mogą mieć dostęp wyłącznie do tych danych, które są im potrzebne do wykonywania ich zadań.

Artykuł 34
Okres przechowywania wpisów

1. Wpisy wprowadzone do SIS zgodnie z niniejszym rozporządzeniem przechowywane są wyłącznie przez okres konieczny dla osiągnięcia celów, w których zostały wprowadzone.

2. Państwo członkowskie, które dokonało wpisu, w terminie pięciu lat od daty jego dokonania w SIS weryfikuje potrzebę jego zachowania.

3. Każde państwo członkowskie ustanawia w stosownych przypadkach krótsze terminy weryfikacji, zgodnie ze swoim prawem krajowym.

4. W przypadkach, gdy personel biura SIRENE odpowiadający za koordynację i weryfikację jakości danych upewni się, że wpis dotyczący osoby spełnił swój cel i powinien zostać usunięty z SIS, personel powiadamia organ, który utworzył wpis, by poddał tę kwestię pod rozwagę. W terminie 30 dni kalendarzowych od otrzymania wspomnianego zgłoszenia organ wskazuje, że wpis został usunięty lub ma zostać usunięty lub określa powody zachowania wpisu. Jeżeli organ nie udzieli odpowiedzi w terminie 30 dni, wpis jest usuwany przez personel biura SIRENE. Biura SIRENE zgłaszają wszelkie powracające problemy w tym obszarze swojemu krajowemu organowi nadzorczemu.

5. W trakcie okresu weryfikacji państwo członkowskie dokonujące wpisu może, na podstawie wszechstronnej i indywidualnej oceny, która podlega rejestracji, podjąć decyzję o dłuższym przechowywaniu wpisu, o ile jest to konieczne do celów, w których wpis ten został dokonany. W takim przypadku ust. 2 ma zastosowanie również do przedłużenia okresu przechowywania. Wszelkie informacje o przedłużeniu okresu przechowywania wpisu są przekazywane do CS-SIS.

6. Po upływie okresu weryfikacji, o którym mowa w ust. 2, wpisy usuwane są automatycznie poza przypadkami, gdy państwo członkowskie, które dokonało wpisu, przekazało do CS-SIS informację o przedłużeniu okresu przechowywania wpisu w CS-SIS zgodnie z ust. 5. CS-SIS automatycznie informuje państwa członkowskie z czteromiesięcznym wyprzedzeniem o zaplanowanym usunięciu danych z systemu.

7. Państwa członkowskie przechowują statystyki dotyczące liczby wpisów, których okres przechowywania został przedłużony zgodnie z ust. 5.

Artykuł 35
Usuwanie wpisów

1. Wpisy dotyczące odmowy wjazdu i pobytu zgodnie z art. 24 usuwa się po wycofaniu przez właściwy organ decyzji, zgodnie z którą wpisu dokonano, w stosownych przypadkach po procedurze konsultacji, o której mowa w art. 26.

2. Wpisy dotyczące obywateli państw trzecich objętych środkiem ograniczającym, o których to wpisach mowa w art. 27, usuwa się po zakończeniu, zawieszeniu lub anulowaniu środka służącego wykonaniu zakazu podróży.

3. Wpisy dotyczące osoby, która uzyskała obywatelstwo któregokolwiek z państw, których obywatele korzystają z prawa do swobodnego przepływu w obrębie Unii, są usuwane po stwierdzeniu lub uzyskaniu przez państwo członkowskie dokonujące wpisu informacji zgodnie z art. 38, że dana osoba uzyskała takie obywatelstwo.

ROZDZIAŁ VIII

OGÓLNE ZASADY PRZETWARZANIA DANYCH

Artykuł 36
Przetwarzanie danych SIS

1. Państwa członkowskie mogą przetwarzać dane, o których mowa w art. 20, do celów odmowy pozwolenia na wjazd i pobyt na ich terytorium.

2. Dane mogą być kopiowane wyłącznie do celów technicznych, pod warunkiem że takie kopiowanie jest niezbędne do przeprowadzenia bezpośredniego wyszukiwania przez organy określone w art. 29. Do takich kopii mają zastosowanie przepisy niniejszego rozporządzenia. Państwo członkowskie nie kopiuje danych zawartych we wpisach ani danych dodatkowych wprowadzonych przez inne państwo członkowskie z N.SIS lub CS-SIS tego państwa do innych krajowych plików danych.

3. Kopie techniczne, o których mowa w ust. 2, przekształcane w bazy danych istniejące w trybie offline mogą być przechowywane przez okres nieprzekraczający 48 godzin. Okres ten może zostać przedłużony w sytuacjach awaryjnych do czasu ich ustania.

   Niezależnie od przepisów akapitu pierwszego, tworzenie kopii technicznych przekształcanych w bazy danych istniejące w trybie offline do użytku organów wizowych jest zakazane, z wyjątkiem kopii sporządzonych do użytku jedynie w sytuacjach awaryjnych, gdy sieć pozostaje niedostępna przez ponad 24 godziny.

   Państwa członkowskie prowadzą aktualny spis takich kopii, który udostępniają ich krajowemu organowi nadzorczemu i zapewniają, by w odniesieniu do tych kopii stosowane były przepisy niniejszego rozporządzenia, a w szczególności przepisy art. 10.

4. Prawo dostępu do danych przyznaje się wyłącznie w granicach kompetencji organów krajowych, o których mowa w art. 29, właściwie upoważnionym pracownikom.

5. Każdy przypadek przetwarzania zawartych w SIS informacji do celów innych niż te, w których wpisy te zostały dokonane w SIS, musi być związany z konkretną sprawą i uzasadniony potrzebą, by zapobiec bezpośredniemu poważnemu zagrożeniu porządku publicznego oraz bezpieczeństwa publicznego, poważnymi względami bezpieczeństwa narodowego lub koniecznością zapobieżenia poważnym przestępstwom. W tym celu wcześniej uzyskuje się zgodę państwa członkowskiego dokonującego wpisu.

6. Dane dotyczące dokumentów odnoszących się do osób wprowadzone zgodnie z art. 38 ust. 2 lit. j) i k) rozporządzenia (UE) 2018/xxx mogą być wykorzystywane przez organy, o których mowa w art. 29 ust. 1 lit. d) zgodnie z prawem każdego państwa członkowskiego.

7. Wszelkie przypadki wykorzystywania danych w sposób niezgodny z ust. 1–6 uznaje się zgodnie z prawem krajowym każdego państwa członkowskiego za nadużycie.

8. Każde państwo członkowskie przekazuje Agencji wykaz swoich właściwych organów, które są upoważnione do bezpośredniego wyszukiwania danych zawartych w SIS zgodnie z niniejszym rozporządzeniem, jak również wszelkie zmiany dotyczące tego wykazu. Wykaz ten określa – z wyszczególnieniem dla każdego organu – jakie dane mogą być wyszukiwane i do jakich celów. Agencja zapewnia coroczne publikowanie wykazu w *Dzienniku Urzędowym Unii Europejskiej*.

9. O ile prawo Unii nie określa szczegółowych przepisów, dane wprowadzane do N.SIS podlegają prawu każdego państwa członkowskiego.

Artykuł 37
Dane SIS a pliki krajowe

1. Artykuł 36 ust. 2 nie narusza prawa państwa członkowskiego do przechowywania w swoich plikach krajowych danych SIS, w związku z którymi podjęto działanie na jego terytorium. Dane takie są przechowywane w plikach krajowych przez okres nie dłuższy niż trzy lata, chyba że przepisy szczegółowe prawa krajowego przewidują dłuższy okres ich przechowywania.

2. Artykuł 36 ust. 2 nie narusza prawa państwa członkowskiego do przechowywania w swoich plikach krajowych danych zawartych w konkretnym wpisie dokonanym w SIS przez to państwo członkowskie.

Artykuł 38
Informacja w przypadku niewykonania wpisu

Jeśli żądane działanie nie może być wykonane, wezwane państwo członkowskie niezwłocznie informuje o tym państwo członkowskie dokonujące wpisu.

Artykuł 39
Jakość danych przetwarzanych w SIS

1. Na państwie członkowskim, które dokonało wpisu, spoczywa obowiązek zapewnienia, by dane były dokładne, aktualne i wprowadzane do SIS zgodnie z prawem.

2. Do zmiany, uzupełniania, korekty, aktualizacji lub usuwania wprowadzonych danych upoważnione jest wyłącznie państwo członkowskie, które dokonało wpisu.

3. Jeżeli państwo członkowskie inne niż to, które dokonało wpisu, posiada dowody wskazujące, że element danych jest niezgodny ze stanem faktycznym lub jest przechowywany niezgodnie z prawem, informuje o tym – w drodze wymiany informacji uzupełniających – państwo członkowskie dokonujące wpisu, możliwie szybko i nie później niż dziesięć dni po stwierdzeniu istnienia takich dowodów. Państwo członkowskie dokonujące wpisu sprawdza te informacje oraz, jeśli to konieczne, niezwłocznie koryguje lub usuwa zakwestionowane dane.

4. Jeżeli państwa członkowskie nie są w stanie osiągnąć porozumienia w terminie dwóch miesięcy od pierwszego dostarczenia dowodów, jak opisano w ust. 3,

państwo członkowskie, które nie dokonało wpisu, przekazuje sprawę zainteresowanym krajowym organom nadzoru w celu wydania decyzji.

5. Jeżeli dana osoba twierdzi, że nie jest osobą poszukiwaną na podstawie wpisu, państwa członkowskie wymieniają informacje uzupełniające. Jeżeli wynik kontroli potwierdza, że rzeczywiście chodzi o dwie różne osoby, osoba ta zostaje powiadomiona o środkach określonych w art. 42.

6. Jeśli istnieje już wpis w SIS dotyczący danej osoby, państwo członkowskie, które dokonuje kolejnego wpisu, uzgadnia jego dokonanie z państwem członkowskim, które dokonało wpisu jako pierwsze. Uzgodnień dokonuje się w drodze wymiany informacji uzupełniających.

Artykuł 40
Incydenty związane z bezpieczeństwem informacji

1. Wszelkie wydarzenia, które mają lub mogą mieć wpływ na bezpieczeństwo SIS oraz mogą spowodować uszkodzenie lub utratę danych SIS, uznaje się za incydent związany z bezpieczeństwem informacji, w szczególności jeżeli mogło dojść do uzyskania dostępu do danych lub jeżeli została lub mogła zostać naruszona dostępność, integralność lub poufność przedmiotowych danych.

2. Incydentami związanymi z bezpieczeństwem informacji zarządza się w taki sposób, aby zapewnić szybkie, skuteczne i właściwe reagowanie.

3. Państwa członkowskie zgłaszają incydenty związane z bezpieczeństwem informacji Komisji, Agencji i Europejskiemu Inspektorowi Ochrony Danych. Agencja zgłasza incydenty związane z bezpieczeństwem informacji Komisji i Europejskiemu Inspektorowi Ochrony Danych.

4. Informacje dotyczące incydentu związanego z bezpieczeństwem informacji, który ma lub może mieć wpływ na funkcjonowanie SIS w państwie członkowskim lub w Agencji lub który ma lub może mieć wpływ na dostępność, integralność i poufność danych wprowadzonych lub przesłanych przez inne państwa członkowskie, przekazuje się państwom członkowskim i zgłasza zgodnie z przekazanym przez Agencję planem zarządzania incydentami.

Artykuł 41
Rozróżnianie osób o podobnych cechach

Jeżeli przy dokonywaniu nowego wpisu stanie się oczywiste, że w SIS istnieje już osoba z takim samym elementem opisu tożsamości, zastosowanie ma następująca procedura:

a) biuro SIRENE zwraca się do organu, który wystosował wniosek o dokonanie wpisu, o wyjaśnienie, czy wpis dotyczy tej samej osoby;

b) jeżeli kontrola potwierdzi, że osoba, której dotyczy nowy wpis, oraz osoba już ujęta w SIS to rzeczywiście ta sama osoba, biuro SIRENE stosuje procedurę dokonywania wielokrotnych wpisów, o której mowa w art. 39 ust. 6. Jeżeli kontrola wykaże, że chodzi o dwie różne osoby, biuro SIRENE przyjmuje

wniosek o dokonanie drugiego wpisu, dodając informacje niezbędne do uniknięcia błędnej identyfikacji.

Artykuł 42
Dodatkowe dane wprowadzane w celu rozwiązywania problemów związanych z przywłaszczeniem tożsamości

1. Jeżeli istnieje ryzyko pomylenia osoby, której faktycznie ma dotyczyć wpis, z osobą, której tożsamość jest przedmiotem przywłaszczenia tożsamości, państwo członkowskie dokonujące wpisu uzupełnia wpis za wyraźną zgodą tej ostatniej osoby o dane dotyczące tej drugiej osoby w celu uniknięcia negatywnych skutków błędnej identyfikacji.

2. Dane osoby, której tożsamość jest przedmiotem przywłaszczenia tożsamości, wykorzystywane są wyłącznie w celu:

   a) umożliwienia właściwym organom odróżnienia osoby, której tożsamość jest przedmiotem przywłaszczenia tożsamości, od osoby, której faktycznie dotyczy wpis;

   b) umożliwienia osobie, której tożsamość jest przedmiotem przywłaszczenia tożsamości, udowodnienia swojej tożsamości i stwierdzenia faktu przywłaszczenia tożsamości.

3. Na użytek niniejszego artykułu jedynie następujące dane osobowe mogą być wprowadzane do SIS i dalej przetwarzane w tym systemie:

   a) nazwisko (nazwiska);

   b) imiona;

   c) nazwisko(-a) rodowe;

   d) poprzednio używane imiona/nazwiska oraz wszelkie aliasy, wpisane oddzielnie, jeśli to możliwe;

   e) wszelkie szczególne obiektywne cechy fizyczne niepodlegające zmianom;

   f) miejsce urodzenia;

   g) data urodzenia;

   h) płeć;

   i) wizerunek twarzy;

   j) odciski palców;

   k) obywatelstwo (obywatelstwa);

   l) kategoria dokumentu tożsamości danej osoby;

m) państwo wydania dokumentu tożsamości danej osoby;

n) numer (numery) dokumentu tożsamości danej osoby;

o) data wydania dokumentu tożsamości danej osoby;

p) adres pokrzywdzonego;

q) imię ojca pokrzywdzonego;

r) imię matki pokrzywdzonego.

4. Techniczne zasady wprowadzania i dalszego przetwarzania danych, o których mowa w ust. 3, określa się w drodze środków wykonawczych określonych i opracowanych zgodnie z procedurą sprawdzającą, o której mowa w art. 55 ust. 2.

5. Dane określone w ust. 3 są usuwane w tym samym czasie, co odpowiadający im wpis, lub wcześniej, jeśli dana osoba zwraca się z takim wnioskiem.

6. Prawo dostępu do danych, o których mowa w ust. 3, przysługuje wyłącznie organom posiadającym prawo dostępu do odpowiadającego im wpisu. Mogą one korzystać z niego wyłącznie w celu uniknięcia błędnej identyfikacji.

Artykuł 43
Odsyłacze do innych wpisów

1. Państwo członkowskie może utworzyć odsyłacz do innych wpisów, których dokonuje w SIS. Celem utworzenia takiego odsyłacza jest ustanowienie związku pomiędzy co najmniej dwoma wpisami.

2. Utworzenie odsyłacza nie wpływa na konkretne działanie, jakie należy podjąć na podstawie każdego z tak połączonych wpisów, ani na okres przechowywania każdego z tak połączonych wpisów.

3. Utworzenie odsyłacza nie wpływa na prawa dostępu przewidziane w niniejszym rozporządzeniu. Organy nieposiadające prawa dostępu do niektórych kategorii wpisów nie mogą widzieć odsyłacza do wpisu, do którego nie mają dostępu.

4. Państwo członkowskie tworzy odsyłacz do innych wpisów, gdy jest to podyktowane potrzebą operacyjną.

5. Jeżeli państwo członkowskie uzna, że utworzenie przez inne państwo członkowskie odsyłacza do innego wpisu jest niezgodne z jego prawem krajowym lub zobowiązaniami międzynarodowymi, może podjąć niezbędne środki, by uniemożliwić dostęp do tego odsyłacza ze swojego terytorium lub uniemożliwić dostęp do niego swoim organom znajdującym się poza jego terytorium.

6. Techniczne zasady tworzenia odsyłaczy do wpisów określa się i opracowuje zgodnie z procedurą sprawdzającą określoną w art. 55 ust. 2.

Artykuł 44
Cel i okres przechowywania informacji uzupełniających

1. Państwa członkowskie przechowują odniesienia do decyzji, które są podstawą wpisu, w biurze SIRENE w celu ułatwienia wymiany informacji uzupełniających.

2. Dane osobowe przechowywane w aktach biura SIRENE w wyniku wymiany informacji są przechowywane wyłącznie przez okres wymagany do osiągnięcia celów, w których zostały dostarczone. Są one usuwane najpóźniej po upływie roku od momentu usunięcia związanego z nimi wpisu z SIS.

3. Ustęp 2 nie narusza prawa państwa członkowskiego do przechowywania w plikach krajowych danych dotyczących poszczególnych wpisów, których samo dokonało, lub wpisów, w związku z którymi podjęto działania na jego terytorium. Okres przechowywania takich danych we wspomnianych plikach reguluje prawo krajowe.

Artykuł 45
Przekazywanie danych osobowych stronom trzecim

Dane przetwarzane w SIS oraz powiązane informacje uzupełniające zgodnie z niniejszym rozporządzeniem nie są przekazywane ani udostępniane państwom trzecim ani organizacjom międzynarodowym.

ROZDZIAŁ IX

OCHRONA DANYCH

Artykuł 46
Mające zastosowanie ustawodawstwo

1. Rozporządzenie (WE) nr 45/2001 stosuje się w odniesieniu do przetwarzania danych osobowych przez Agencję na mocy niniejszego rozporządzenia.

2. Rozporządzenie 2016/679 stosuje się w odniesieniu do przetwarzania danych osobowych przez organy, o których mowa w art. 29 niniejszego rozporządzenia, pod warunkiem że zastosowania nie mają przepisy krajowe transponujące dyrektywę (UE) 2016/680.

3. W przypadku przetwarzania danych przez właściwe organy krajowe do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym zapobiegania zagrożeniom dla bezpieczeństwa publicznego, zastosowanie mają przepisy krajowe transponujące dyrektywę (UE) 2016/680.

Artykuł 47

Prawo dostępu, poprawianie nieścisłości oraz usuwanie danych przechowywanych niezgodnie z prawem

1. Prawo osób, których dane dotyczą, do dostępu do danych na ich temat wprowadzonych do SIS oraz do poprawy lub usunięcia takich danych wykonuje się zgodnie z prawem państwa członkowskiego, wobec którego powołują się one na to prawo.

2. Jeżeli prawo krajowe tak stanowi, krajowy organ nadzorczy decyduje o tym, czy informacje mają być podane do wiadomości oraz o sposobie ich podawania.

3. Państwo członkowskie, inne niż to, które dokonało wpisu, może przekazać informację dotyczącą takich danych tylko w przypadku, gdy uprzednio umożliwiło państwu członkowskiemu dokonującemu wpisu zajęcie w tej sprawie stanowiska. Umożliwienie zajęcia stanowiska następuje w drodze wymiany informacji uzupełniających.

4. Państwo członkowskie podejmuje decyzję o nieprzekazywaniu całości lub części informacji osobie, której dane dotyczą, zgodnie z prawem krajowym, w takim zakresie oraz przez tak długo, jak częściowe lub całkowite ograniczenie stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym, przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów osoby fizycznej, której dane dotyczą, aby:

   a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;

   b) unikać utrudniania zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar;

   c) chronić bezpieczeństwo publiczne;

   d) chronić bezpieczeństwo narodowe;

   e) chronić prawa i wolności innych osób.

5. Dana osoba informowana jest możliwie szybko, a w każdym razie nie później niż 60 dni od daty złożenia przez nią wniosku o dostęp, lub wcześniej, jeżeli prawo krajowe przewiduje krótszy okres.

6. O działaniach podjętych po skorzystaniu przez zainteresowanego z jego prawa do wystąpienia o poprawę i usunięcie danych informuje się go możliwie jak najszybciej, a w każdym przypadku nie później niż 3 miesiące od daty złożenia przez niego wniosku o poprawę lub usunięcie danych lub wcześniej, jeżeli prawo krajowe tak stanowi.

Artykuł 48
Prawo do informacji

1. Obywatele państwa trzeciego, których dotyczy wpis dokonany zgodnie z niniejszym rozporządzeniem, otrzymują informacje o wpisie zgodnie z art. 10 i 11 dyrektywy 95/46/WE. Informacje te są przekazywane na piśmie wraz z kopią decyzji krajowej, o której mowa w art. 24 ust. 1 i która stanowi podstawę dokonania wpisu lub wraz z odesłaniem do takiej decyzji.

2. Informacje te w żadnym przypadku nie są przekazywane,

   a) jeżeli:

      i) dane osobowe nie zostały uzyskane od danego obywatela państwa trzeciego;

      oraz

      ii) przekazanie tych informacji okazuje się niemożliwe lub wymagałoby nieproporcjonalnego nakładu pracy;

   b) jeżeli dany obywatel państwa trzeciego posiada już te informacje;

   c) jeżeli prawo krajowe pozwala ograniczyć prawo do informacji, w szczególności ze względu na ochronę bezpieczeństwa narodowego, obronność kraju, bezpieczeństwo publiczne oraz w celu przeciwdziałania przestępstwom oraz ich wykrywania, ścigania i karania.

Artykuł 49
Środki odwoławcze

1. Każdy może wystąpić do sądów lub organów właściwych na mocy prawa krajowego któregokolwiek z państw członkowskich z wnioskiem o dostęp do informacji, poprawienie, skreślenie lub usunięcie informacji lub o odszkodowanie w związku z dotyczącym go wpisem.

2. Państwa członkowskie zobowiązują się wzajemnie do wykonywania ostatecznych decyzji wydanych przez sądy lub organy, o których mowa w ust. 1 niniejszego artykułu, bez uszczerbku dla przepisów art. 53.

3. Aby uzyskać spójny przegląd funkcjonowania środków odwoławczych, wzywa się krajowe organy nadzorcze do opracowania standardowego systemu statystycznego na potrzeby corocznej sprawozdawczości w zakresie:

   a) liczby wniosków o uzyskanie dostępu przekazanych administratorowi danych przez osoby, których dane dotyczą, oraz liczby przypadków, w których przyznano dostęp do danych;

   b) liczby wniosków o uzyskanie dostępu przekazanych krajowemu organowi nadzorczemu przez osoby, których dane dotyczą, oraz liczby przypadków, w których przyznano dostęp do danych;

c) liczby wniosków o poprawę nieścisłości oraz o usunięcie danych przechowywanych niezgodnie z prawem przekazanych administratorowi danych oraz liczby przypadków, w których dane zostały poprawione lub usunięte;

d) liczby wniosków o poprawę nieścisłości oraz o usunięcie danych przechowywanych niezgodnie z prawem przekazanych krajowemu organowi nadzorczemu;

e) liczby spraw rozpatrzonych przez sądy;

f) liczby spraw, w których sąd orzekł na korzyść strony skarżącej w dowolnym aspekcie sprawy;

g) jakichkolwiek uwag dotyczących przypadków wzajemnego uznawania orzeczeń kończących postępowanie w sprawie wydanych przez sądy lub organy innych państw członkowskich w odniesieniu do wpisów utworzonych przez państwo członkowskie dokonujące wpisu.

Sprawozdania krajowych organów nadzoru przekazuje się do mechanizmu współpracy określonego w art. 52.

Artykuł 50
Nadzór nad N.SIS

1. Każde państwo członkowskie zapewnia, by niezależny krajowy organ nadzorczy lub niezależne krajowe organy nadzorcze wyznaczone w każdym państwie członkowskim, którym powierzono uprawnienia określone w rozdziale VI dyrektywy (UE) 2016/680 lub w rozdziale VI rozporządzenia (UE) 2016/679, niezależnie nadzorowały, czy dane osobowe zawarte w SIS są przetwarzane na jego terytorium i przekazywane z jego terytorium zgodnie z prawem, a także wymianę i dalsze przetwarzanie informacji uzupełniających.

2. Krajowy organ nadzorczy zapewnia, aby co najmniej co cztery lata przeprowadzany był audyt operacji przetwarzania danych w ramach ich N.SIS zgodny z międzynarodowymi standardami audytu. Audyt jest prowadzony przez krajowe organy nadzorcze albo krajowe organy nadzorcze bezpośrednio zlecają przeprowadzenie audytu niezależnemu audytorowi ds. ochrony danych. Krajowy organ nadzorczy zawsze zachowuje kontrolę nad obowiązkami niezależnego audytora i podejmuje jego obowiązki.

3. Państwa członkowskie zapewniają, by krajowy organ nadzorczy dysponował zasobami wystarczającymi do wykonania zadań powierzonych mu na mocy niniejszego rozporządzenia.

Artykuł 51
Nadzór nad Agencją

1. Europejski Inspektor Ochrony Danych zapewnia, by działania Agencji w zakresie przetwarzania danych osobowych były wykonywane zgodnie z niniejszym

rozporządzeniem. Zastosowanie mają odpowiednio obowiązki i uprawnienia określone w art. 46 i 47 rozporządzenia (WE) nr 45/2001.

2. Europejski Inspektor Ochrony Danych zapewnia, by co najmniej co cztery lata przeprowadzany był audyt działań Agencji w zakresie przetwarzania danych osobowych zgodny z międzynarodowymi standardami audytu. Sprawozdanie z tego audytu przesyłane jest Parlamentowi Europejskiemu, Radzie, Agencji, Komisji i krajowym organom nadzorczym. Przed przyjęciem sprawozdania Agencji umożliwia się przedstawienie uwag.

Artykuł 52
Współpraca krajowych organów nadzorczych i Europejskiego Inspektora Ochrony Danych

1. Krajowe organy nadzorcze oraz Europejski Inspektor Ochrony Danych, działając w ramach swoich kompetencji, współpracują czynnie w ramach swoich zadań i zapewniają skoordynowany nadzór nad SIS.

2. W zależności od potrzeb i w ramach swoich kompetencji obie strony wymieniają istotne informacje, wspomagają się wzajemnie w przeprowadzaniu audytów i inspekcji, analizują trudności w zakresie wykładni lub stosowania niniejszego rozporządzenia oraz innych wiążących aktów prawnych UE, badają problemy, które wykryto w wyniku sprawowania niezależnego nadzoru lub w związku z wykonywaniem praw osób, których dotyczą dane, sporządzają uzgodnione wnioski w sprawie wspólnych rozwiązań problemów oraz upowszechniają wiedzę o uprawnieniach w zakresie ochrony danych.

3. W celach określonych w ust. 2 krajowe organy nadzorcze oraz Europejski Inspektor Ochrony Danych spotykają się co najmniej dwa razy w roku w ramach Europejskiej Rady Ochrony Danych ustanowionej rozporządzeniem (UE) 2016/679. Koszty tych posiedzeń ponosi i ich obsługę prowadzi Rada ustanowiona rozporządzeniem (UE) 2016/679. Podczas pierwszego spotkania zostaje przyjęty regulamin wewnętrzny. Dalsze metody pracy opracowywane są wspólnie, w zależności od potrzeb.

4. Wspólne sprawozdanie z działalności dotyczącej skoordynowanego nadzoru przesyłane jest przez Radę ustanowioną rozporządzeniem (UE) 2016/679 co dwa lata Parlamentowi Europejskiemu, Radzie i Komisji.

ROZDZIAŁ X

ODPOWIEDZIALNOŚĆ

Artykuł 53
Odpowiedzialność

1. Każde państwo członkowskie ponosi odpowiedzialność za wszelkie szkody wyrządzone danej osobie w związku z użytkowaniem N.SIS. Przepis ten ma również zastosowanie do szkód wyrządzonych przez państwo członkowskie dokonujące

wpisu, jeżeli państwo to wprowadziło dane niezgodne ze stanem faktycznym lub przechowuje dane w sposób niezgodny z prawem.

2. Jeżeli państwo członkowskie, przeciwko któremu wniesione zostało powództwo, nie jest państwem członkowskim dokonującym wpisu, to państwo dokonujące wpisu jest zobowiązane do zwrotu, na wniosek państwa pozwanego, wypłaconego odszkodowania, chyba że państwo członkowskie domagające się zwrotu korzystało z przedmiotowych danych z naruszeniem niniejszego rozporządzenia.

3. W przypadku naruszenia przez państwo członkowskie swoich obowiązków wynikających z niniejszego rozporządzenia i spowodowania tym samym szkody w SIS, ponosi ono odpowiedzialność za tę szkodę, chyba że Agencja lub inne państwo członkowskie uczestniczące w SIS nie podjęły rozsądnych kroków, by zapobiec wystąpieniu szkody lub zminimalizować jej rozmiaru.

ROZDZIAŁ XI

PRZEPISY KOŃCOWE

Artykuł 54
Monitorowanie i statystyka

1. Agencja zapewnia, by wprowadzono procedury pozwalające kontrolować, na ile SIS służy swojemu przeznaczeniu pod kątem wyników, opłacalności, bezpieczeństwa i jakości usług.

2. Do celów prac konserwacyjno-technicznych, przygotowywania sprawozdań i sporządzania statystyk Agencja posiada dostęp do niezbędnych informacji związanych z operacjami przetwarzania danych wykonywanymi w centralnym SIS.

3. Agencja sporządza dzienne, miesięczne i roczne statystyki pokazujące liczbę rekordów przypadających na daną kategorię wpisów, liczbę uzyskanych rocznie trafień przypadających na daną kategorię wpisów, liczbę wyszukiwań SIS oraz liczbę wejść do SIS w celu wprowadzenia, zaktualizowania lub usunięcia wpisu ogółem oraz w rozbiciu na poszczególne państwa członkowskie, w tym statystyki dotyczące procedury konsultacji, o której mowa w art. 26. Statystyki te nie zawierają żadnych danych osobowych. Roczne sprawozdanie statystyczne podlega publikacji.

4. Państwa członkowskie oraz Europol i Europejska Agencja Straży Granicznej i Przybrzeżnej przekazują Agencji i Komisji informacje niezbędne do sporządzenia sprawozdań, o których mowa w ust. 7 i 8.

5. Agencja przekazuje państwom członkowskim, Komisji, Europolowi i Europejskiej Agencji Straży Granicznej i Przybrzeżnej opracowane przez siebie sprawozdania statystyczne. Aby móc monitorować wdrażanie unijnych aktów prawnych, Komisja może zwrócić się do Agencji o regularne sporządzanie lub sporządzenie *ad hoc*

dodatkowych szczegółowych sprawozdań statystycznych dotyczących działania lub korzystania z łączności SIS i SIRENE.

6. Do celów ust. 3–5 niniejszego artykułu i art. 15 ust. 5 Agencja ustanawia, wdraża i obsługuje w swoich obiektach technicznych centralne repozytorium zawierające dane wymienione w ust. 3 niniejszego artykułu i w art. 15 ust. 5, które uniemożliwi identyfikację osób fizycznych i umożliwi Komisji oraz organom wymienionym w ust. 5 uzyskanie dostosowanych do ich potrzeb sprawozdań i statystyk. Agencja udziela państwom członkowskim, Komisji, Europolowi i Europejskiej Agencji Straży Granicznej i Przybrzeżnej dostępu do centralnego repozytorium w drodze bezpiecznego dostępu za pośrednictwem infrastruktury łączności wyposażonej w kontrolę dostępu oraz specjalne profile użytkownika służące wyłącznie do celów sporządzania sprawozdań i statystyk.

   Szczegółowe zasady dotyczące funkcjonowania centralnego repozytorium i zasady ochrony i bezpieczeństwa danych mające zastosowanie do repozytorium określa się i opracowuje w drodze środków wykonawczych przyjętych zgodnie z procedurą sprawdzającą, o której mowa w art. 55 ust. 2.

7. Dwa lata po rozpoczęciu eksploatacji SIS, a następnie co dwa lata Agencja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące technicznej sprawności centralnego SIS i infrastruktury łączności, w tym ich bezpieczeństwa, oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi.

8. Trzy lata po rozpoczęciu eksploatacji SIS, a następnie co cztery lata Komisja sporządza ogólną ocenę centralnego SIS oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi. W takiej ogólnej ocenie zawiera się analizę osiągniętych wyników w zestawieniu z celami i określa się, na ile wciąż aktualne są pierwotne przesłanki, w jaki sposób niniejsze rozporządzenie stosowane jest do centralnego SIS, na ile bezpieczny jest centralny SIS i jakie będą konsekwencje dla przyszłych operacji. Komisja przekazuje ocenę Parlamentowi Europejskiemu i Radzie.

Artykuł 55
Procedura komitetowa

1. Komisję wspomaga komitet. Komitet jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 56

Zmiany w rozporządzeniu (UE) nr 515/2014

W rozporządzeniu (UE) nr 515/2014[74] wprowadza się następujące zmiany:

W art. 6 dodaje się ust. 6 w brzmieniu:

„6. Podczas fazy opracowywania państwa członkowskie oprócz podstawowego przydziału środków otrzymują dodatkowy przydział w wysokości 36,8 mln EUR przyznawany w formie płatności ryczałtowej, który ma zostać w całości przeznaczony na krajowe systemy SIS w celu zapewnienia ich szybkiej i efektywnej modernizacji zgodnie z wdrażaniem centralnego SIS zgodnie z wymogami rozporządzenia (UE) 2018/…[*] i rozporządzenia (UE) 2018/…[**].

[*]*Rozporządzenie w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych oraz rozporządzenie (Dz.U.…).*

[**]Rozporządzenie (UE) 2018/…w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych oraz rozporządzenie (Dz.U…..).”.

Artykuł 57
Uchylenie

Rozporządzenie (WE) nr 1987/2006 w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II).

Decyzja Komisji 2010/261/UE z dnia 4 maja 2010 r. w sprawie planu bezpieczeństwa dla centralnego systemu SIS II i infrastruktury łączności[75].

Artykuł 25 konwencji wykonawczej do układu z Schengen[76].

Artykuł 58
Wejście w życie i stosowanie

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.

2. Niniejsze rozporządzenie stosuje się od daty ustalonej przez Komisję po:

   a) przyjęciu niezbędnych środków wykonawczych;

   b) powiadomieniu Komisji przez państwa członkowskie o zakończeniu niezbędnych technicznych i prawnych przygotowań do przetwarzania danych SIS oraz wymiany informacji uzupełniających zgodnie z niniejszym rozporządzeniem;

---

74 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 515/2014 z dnia 16 kwietnia 2014 r. ustanawiające, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument na rzecz wsparcia finansowego w zakresie granic zewnętrznych i wiz (Dz.U. L 150 z 20.5.2014, s. 143).

75 Decyzja Komisji nr 2010/261/UE z dnia 4 maja 2010 r. w sprawie planu bezpieczeństwa dla centralnego systemu SIS II i infrastruktury łączności (Dz.U. L 112 z 5.5.2010, s. 31).

76 Dz.U. L 239 z 22.9.2000, s. 19.

c) powiadomieniu Komisji przez Agencję o zakończeniu wszystkich badań w zakresie CS-SIS i interakcji między CS-SIS a N.SIS.

3. Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich zgodnie z Traktatem o funkcjonowaniu Unii Europejskiej.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

1.2. Dziedziny polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa

1.3. Charakter wniosku/inicjatywy

1.4. Cele

1.5. Uzasadnienie wniosku/inicjatywy

1.6. Okres trwania działania i jego wpływ finansowy

1.7. Przewidywane tryby zarządzania

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

2.2. System zarządzania i kontroli

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

3.2.2. Szacunkowy wpływ na środki operacyjne

3.2.3. Szacunkowy wpływ na środki administracyjne

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

3.2.5. Udział osób trzecich w finansowaniu

3.3. Szacunkowy wpływ na dochody

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek – ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, uchylające rozporządzenie (WE) nr 1987/2006

1.2. Dziedziny polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa[77]

Dziedzina polityki: Migracja i sprawy wewnętrzne (tytuł 18)

1.3. Charakter wniosku/inicjatywy

☐ Wniosek/inicjatywa dotyczy **nowego działania**

☐ Wniosek/inicjatywa dotyczy **nowego działania będącego następstwem projektu pilotażowego/działania przygotowawczego**[78]

☑ Wniosek/inicjatywa wiąże się z **przedłużeniem bieżącego działania**

☐ Wniosek/inicjatywa dotyczy **działania, które zostało przekształcone pod kątem nowego działania**

1.4. Cele

1.4.1. Wieloletnie cele strategiczne Komisji wskazane we wniosku/inicjatywie

Cel – „W kierunku nowej polityki migracyjnej”

Komisja wielokrotnie podkreślała konieczność zrewidowania podstawy prawnej SIS w celu podjęcia nowych wyzwań związanych z bezpieczeństwem i migracją. W Europejskim programie w zakresie migracji[79] Komisja stwierdziła na przykład, że skuteczniejsze zarządzanie granicami wymaga lepszego wykorzystania możliwości stwarzanych przez systemy i technologie informatyczne. W Europejskiej agendzie bezpieczeństwa[80] Komisja ogłosiła, że w latach 2015–2016 ma zamiar przeprowadzić ocenę SIS oraz że zbada możliwości wspierania państw członkowskich w wykonywaniu zakazów podróżowania wydanych na szczeblu krajowym. W unijnym planie działania na rzecz zwalczania przemytu migrantów[81] Komisja stwierdziła, że rozważa zobowiązanie organów państw członkowskich do

[77] ABM: *activity-based management*: zarządzanie kosztami działań; ABB: *activity-based budgeting*: budżet zadaniowy.

[78] O którym mowa w art. 54 ust. 2 lit. a) lub b) rozporządzenia finansowego.

[79] COM(2015) 240 final.

[80] COM(2015) 185 final.

[81] COM(2015) 285 final.

wprowadzenia do SIS wszystkich zakazów wjazdu, aby umożliwić ich wykonywanie na skalę unijną. Komisja ogłosiła ponadto, że rozważy kwestię możliwości i proporcjonalności wprowadzania do SIS decyzji nakazujących powrót wydanych przez państwa członkowskie, aby sprawdzać, czy zatrzymany nielegalny migrant podlega decyzji nakazującej powrót w innym państwie członkowskim. Wreszcie w komunikacie w sprawie sprawniejszych i bardziej inteligentnych systemów informacyjnych do celów zarządzania granicami i zapewnienia bezpieczeństwa[82] Komisja podkreśliła, że bada możliwe dodatkowe funkcje SIS w celu przedstawienia wniosków w sprawie zmiany podstawy prawnej systemu.

W wyniku ogólnej oceny systemu i z zachowaniem pełnej zgodności z wieloletnimi celami Komisji wyrażonymi w wyżej wymienionych komunikatach i Planie Strategicznym na lata 2016–2020 DG ds. Migracji i Spraw Wewnętrznych[83] celem niniejszego wniosku jest reforma struktury, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych.

1.4.2. Cele szczegółowe i działania ABM/ABB, których dotyczy wniosek/inicjatywa

Cel szczegółowy nr:

Plan Zarządzania na 2017 r. DG ds. Migracji i Spraw Wewnętrznych – cel szczegółowy nr 1.2:

Skuteczne zarządzanie granicami – ratowanie ludzkiego życia i zabezpieczenie granic zewnętrznych UE

Działania ABM/ABB, których dotyczy wniosek/inicjatywa

Rozdział 18 02 – Bezpieczeństwo wewnętrzne

[82] COM(2016) 205 final.
[83] Ares(2016)2231546 – 12/05/2016.

1.4.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Główne cele polityki wyszczególniono poniżej.

1) Sprzyjanie wysokiemu poziomowi bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej.

2) Zwiększenie skuteczności i wydajności kontroli granicznych.

W wyniku ogólnej oceny SIS dokonanej przez DG HOME w latach 2015–2016 zalecono wprowadzenie usprawnień technicznych systemu i harmonizację krajowych procedur w dziedzinie zarządzania odmowami wjazdu i pobytu. Na przykład aktualne rozporządzenie SIS II jedynie zezwala państwom członkowskim na dokonywanie w SIS wpisów dotyczących odmowy wjazdu i pobytu – ale tego nie wymaga. Niektóre państwa członkowskie systematycznie wpisują wszystkie zakazy wjazdu do SIS, podczas gdy inne tego nie robią. W związku z tym niniejszy wniosek przyczyni się do osiągnięcia wyższego stopnia harmonizacji w tym obszarze poprzez wprowadzenie obowiązku wpisywania do SIS wszystkich zakazów wjazdu, określenie wspólnych zasad dokonywania takich wpisów w systemie oraz określenie przyczyn dokonania wpisu.

W nowym wniosku wprowadzono środki, które stanowią odpowiedź na potrzeby operacyjne i techniczne użytkowników końcowych. W szczególności nowe pola danych dla istniejących wpisów umożliwią funkcjonariuszom straży granicznej uzyskanie wszystkich informacji, których potrzebują, aby efektywnie wykonywać swoje zadania. Co więcej, we wniosku wyraźnie podkreślono znaczenie niezakłóconej dostępności SIS, ponieważ przestoje mogą mieć znaczący wpływ na możliwość prowadzenia kontroli na granicach zewnętrznych. Niniejszy wniosek będzie zatem miał bardzo pozytywny wpływ na skuteczność kontroli granicznych.

Przyjęcie i wdrożenie tych wniosków wpłynie również pozytywnie na ciągłość działania – państwa członkowskie będą miały obowiązek posiadania pełnej lub częściowej kopii krajowej i jej kopii zapasowej. Dzięki temu system będzie w pełni funkcjonalny i operacyjny dla funkcjonariuszy pracujących w terenie.

1.4.4. Wskaźniki wyników i wpływu

Należy określić wskaźniki, które umożliwią monitorowanie realizacji wniosku/inicjatywy.

W trakcie modernizacji systemu:

Po zatwierdzeniu projektu wniosku i przyjęciu specyfikacji technicznych SIS zostanie poddany modernizacji w celu lepszej harmonizacji procedur krajowych na potrzeby użytkowania systemu, poszerzenia zakresu stosowania systemu przez podniesienie poziomu informacji dostępnych dla użytkowników końcowych w celu lepszego informowania funkcjonariuszy przeprowadzających kontrole oraz wprowadzenia zmian technicznych służących podniesieniu bezpieczeństwa i ograniczeniu obciążeń administracyjnych. Zarządzanie projektem modernizacji systemu będzie koordynować Eu-LISA. Ustanowi ona też struktury zarządcze projektu i opracuje szczegółowy harmonogram, określając jednocześnie główne

etapy wdrażania proponowanych zmian, co pozwoli Komisji na uważne monitorowanie procesu wdrażania wniosku.

Cel szczegółowy – Uruchomienie zaktualizowanych funkcji SIS w 2020 r.

Wskaźnik – pomyślne ukończenie fazy testowej zmienionego systemu.

Z chwilą rozpoczęcia funkcjonowania systemu:

Z chwilą rozpoczęcia funkcjonowania systemu eu-LISA zapewni, by wprowadzono procedury pozwalające kontrolować, na ile SIS służy swojemu przeznaczeniu pod kątem wyników, opłacalności, bezpieczeństwa i jakości usług. Dwa lata po rozpoczęciu eksploatacji SIS, a następnie co dwa lata eu-LISA ma obowiązek przedkładać Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące technicznej sprawności centralnego SIS i infrastruktury łączności, w tym ich bezpieczeństwa, oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi. Ponadto eu-LISA sporządza dziennie, miesięczne i roczne statystyki pokazujące liczbę rekordów przypadających na daną kategorię wpisów, liczbę uzyskanych rocznie trafień przypadających na daną kategorię wpisów, liczbę wyszukiwań SIS oraz liczbę wejść do systemu w celu wprowadzenia, zaktualizowania lub usunięcia wpisu ogółem oraz w rozbiciu na poszczególne państwa członkowskie.

Trzy lata po rozpoczęciu eksploatacji SIS, a następnie co cztery lata Komisja sporządza ogólną ocenę centralnego SIS oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi. W takiej ogólnej ocenie zawiera się analizę osiągniętych wyników w zestawieniu z celami i określa się, na ile wciąż aktualne są pierwotne przesłanki, w jaki sposób niniejsze rozporządzenie stosowane jest do centralnego SIS, na ile bezpieczny jest centralny SIS i jakie będą konsekwencje dla przyszłych operacji. Komisja przekazuje ocenę Parlamentowi Europejskiemu i Radzie.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej

1. Sprzyjanie utrzymaniu wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej.

2. Umocnienie walki z międzynarodową przestępczością, terroryzmem i innymi zagrożeniami dla bezpieczeństwa.

3. Rozszerzenie zakresu stosowania SIS poprzez wprowadzenie nowych elementów do wpisów dotyczących odmowy wjazdu i pobytu.

4. Zwiększenie skuteczności odpraw granicznych.

5. Zwiększenie skuteczności prac straży granicznej i organów imigracyjnych.

6. Osiągnięcie wyższego stopnia skuteczności i harmonizacji procedur krajowych oraz zapewnienie wykonalności zakazów wjazdu w całej strefie Schengen.

7. Wkład w walkę z nielegalną migracją.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej

SIS stanowi główną bazę danych bezpieczeństwa w Europie. W związku z brakiem kontroli na granicach wewnętrznych skuteczna walka z przestępczością i terroryzmem zyskała wymiar europejski. SIS jest w związku z tym niezbędny do wspierania kontroli granic zewnętrznych i kontroli nielegalnych migrantów, którzy przebywają na terytoriach krajowych. Cele wniosku dotyczą usprawnień technicznych służących zwiększeniu skuteczności i efektywności systemu oraz lepszej harmonizacji na potrzeby jego użytkowania we wszystkich uczestniczących państwach członkowskich. Transgraniczny charakter wymienionych celów i wyzwań związanych z zapewnieniem skutecznej wymiany informacji w celu zwalczania coraz bardziej różnorodnych zagrożeń oznacza, że UE jest najbardziej odpowiednim podmiotem, by zaproponować rozwiązania kwestii opisanych powyżej. Cele związane z podnoszeniem skuteczności i lepszą harmonizacją na potrzeby użytkowania SIS, a mianowicie zwiększenie wolumenu, jakości i szybkości wymiany informacji za pośrednictwem scentralizowanego systemu danych działającego na dużą skalę i zarządzanego przez agencję regulacyjną (eu-LISA), nie mogą zostać osiągnięte na szczeblu poszczególnych państw członkowskich i wymagają ingerencji na poziomie UE. Jeżeli obecne problemy nie zostaną rozwiązane, SIS będzie nadal funkcjonować na zasadach stosowanych obecnie, co spowoduje utratę szansy na zmaksymalizowanie jego skuteczności i europejskiej wartości dodanej, którą wykazano w wyniku oceny SIS oraz jego użytkowania przez państwa członkowskie.

W samym 2015 r. organy krajowe wysłały do SIS prawie 2,9 mld zapytań i wymieniły ponad 1,8 mln informacji uzupełniających. Wyraźnie pokazuje to istotny wkład systemu w kontrolę granic zewnętrznych. Tak wysoki poziom wymiany informacji między państwami członkowskimi nie zostałby osiągnięty za pomocą rozwiązań zdecentralizowanych, a uzyskanie takich wyników byłoby niemożliwe na szczeblu krajowym. Co więcej, SIS okazał się niezwykle efektywnym narzędziem wymiany informacji do celów walki z terroryzmem i wnosi europejską wartość dodaną, ponieważ pozwala służbom bezpieczeństwa narodowego na szybką, poufną i skuteczną współpracę. Nowe wnioski przyczynią się do dalszego usprawniania wymiany informacji i współpracy między organami państw członkowskich UE odpowiedzialnymi za kontrolę graniczną. Ponadto Europol i Europejska Straż Graniczna i Przybrzeżna, w ramach swoich uprawnień, otrzymają pełny dostęp do systemu, co będzie stanowić jasny wyraz wartości dodanej zaangażowania UE.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

W niniejszej sekcji przedstawiono najważniejsze wnioski wyciągnięte z rozwoju Systemu Informacyjnego Schengen drugiej generacji.

1. Faza opracowywania powinna rozpocząć się dopiero po określeniu wszystkich potrzeb technicznych i operacyjnych. Faza opracowywania może rozpocząć się dopiero po tym, jak ostatecznie przyjęte zostaną podstawowe instrumenty prawne wskazujące cel, zakres stosowania, funkcje i szczegółowe dane techniczne systemu.

2. Komisja przeprowadziła (i dalej prowadzi) częste konsultacje z odpowiednimi zainteresowanymi stronami, w tym z delegatami z Komitetu SIS–VIS w ramach procedury komitetowej. Komitet ten składa się z przedstawicieli państw członkowskich zajmujących się zarówno operacyjnymi kwestiami dotyczącymi SIRENE (współpraca transgraniczna w odniesieniu do SIS) oraz kwestiami technicznymi z zakresu opracowania i utrzymania SIS, jak również powiązanego z nim zastosowania SIRENE. Zmiany zaproponowane w przedmiotowym rozporządzeniu kompleksowo przedyskutowano przy zapewnieniu przejrzystości omawianych kwestii na specjalnie poświęconych temu spotkaniach i warsztatach. Ponadto w ramach swoich struktur wewnętrznych Komisja ustanowiła międzyresortową grupę sterującą składającą się z przedstawicieli Sekretariatu Generalnego, Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych, Dyrekcji Generalnej ds. Sprawiedliwości i Konsumentów, Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa oraz Dyrekcji Generalnej ds. Informatyki. Grupa sterująca monitorowała proces oceny i w razie potrzeby udzielała wytycznych.

3. Komisja dążyła również do uzyskania wiedzy fachowej zewnętrznych ekspertów w ramach trzech badań, których ustalenia uwzględniono przy opracowywaniu niniejszego wniosku:

- oceny technicznej SIS (Kurt Salmon) – w wyniku oceny wskazano główne problemy związane z SIS i przyszłe potrzeby, które należy mieć na uwadze; określono obawy związane z maksymalizacją ciągłości działania i zapewnieniem możliwości dostosowania całej architektury do coraz większych wymogów dotyczących zdolności;

- oceny wpływu technologii informacyjno-komunikacyjnych na potencjalne usprawnienia w architekturze SIS II (Kurt Salmon) – w badaniu ocenie poddano bieżący koszt funkcjonowania SIS na szczeblu krajowym oraz przeanalizowano trzy możliwe scenariusze techniczne mające na celu poprawę systemu. We wszystkich scenariuszach zakłada się przedstawienie zestawu technicznych wniosków koncentrujących się na poprawie systemu centralnego i ogólnej struktury;

- badania dotyczącego wykonalności i skutków ustanowienia w ramach Systemu Informacyjnego Schengen ogólnounijnego systemu wymiany danych dotyczących monitorowania przestrzegania decyzji nakazujących powrót (PwC).W badaniu tym oceniono wykonalność oraz techniczne i operacyjne skutki proponowanych zmian do SIS mających na celu usprawnienie jego stosowania w odniesieniu do powrotów nielegalnych migrantów i zapobiegania ponownemu wjazdowi tych migrantów.

1.5.4. Spójność z innymi właściwymi instrumentami oraz możliwa synergia

Niniejszy wniosek należy postrzegać jako wdrożenie działań, o których mowa w komunikacie z dnia 6 kwietnia 2016 r. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa”[84]. W komunikacie tym podkreślono potrzebę wzmocnienia i usprawnienia przez UE jej systemów informatycznych, struktury danych i wymiany informacji w obszarze ścigania przestępstw, walki z terroryzmem i zarządzania granicami.

[84] COM(2016) 205 final.

Wniosek jest ponadto spójny z szeregiem polityk Unii w tej dziedzinie. Polityki te to:

a) bezpieczeństwo wewnętrzne w odniesieniu do roli SIS w uniemożliwianiu wjazdu obywateli państw trzecich stwarzających zagrożenie bezpieczeństwa;

b) ochrona danych w zakresie, w jakim w niniejszym wniosku zapewnia się ochronę praw podstawowych do poszanowania życia prywatnego osób fizycznych, których dane osobowe są przetwarzane w SIS.

Niniejszy wniosek jest również zgodny z obowiązującymi przepisami Unii, które dotyczą:

a) skutecznej polityki powrotowej UE przyczyniającej się do wzmacniania systemu UE w zakresie wykrywania przypadków ponownego wjazdu obywateli państw trzecich po powrocie i zapobiegania takim przypadkom. Przyczyni się to ograniczenia zachęt dla nielegalnej migracji do UE, co jest jednym z głównych celów Europejskiego programu w zakresie migracji[85];b) **Europejskiej Straży Granicznej i Przybrzeżnej[86]:** w odniesieniu do możliwości przeprowadzania przez pracowników Agencji analiz ryzyka oraz w odniesieniu do zespołów Europejskiej Straży Granicznej i Przybrzeżnej, zespołów składających się z personelu realizującego zadania w dziedzinie powrotów oraz członków zespołów wspierających zarządzanie migracjami, aby osoby te miały prawo, w ramach swojego mandatu, do uzyskania dostępu do danych wprowadzanych do SIS oraz do wyszukiwania tego rodzaju danych;

c) **zarządzania granicami zewnętrznymi** w zakresie, w jakim niniejsze rozporządzenie wspiera poszczególne państwa członkowskie w kontroli ich odcinków granic zewnętrznych UE oraz w budowaniu zaufania do skuteczności unijnego systemu zarządzania granicami;

d) Europolu w zakresie, w jakim w niniejszym wniosku Europolowi udziela się dodatkowych praw, w granicach jego mandatu, do dostępu do danych wprowadzanych do SIS i do wyszukiwania tego rodzaju danych.

Wniosek jest również zgodny z przepisami Unii, które będą obowiązywać w przyszłości i dotyczyć:

a) **systemu wjazdu/wyjazdu[87]**, w ramach którego zaproponowano wykorzystanie połączenia odcisków palców i wizerunku twarzy jako identyfikatorów

85 COM(2015) 240 final.

86 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624 z dnia 14 września 2016 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej oraz zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 i uchylające rozporządzenie (WE) nr 863/2007 Parlamentu Europejskiego i Rady, rozporządzenie Rady (WE) nr 2007/2004 i decyzję Rady 2005/267/WE (Dz.U. L 251 z 16.9.2016, s. 1).

87 Wniosek: rozporządzenie Parlamentu Europejskiego i Rady ustanawiające system wjazdu/wyjazdu w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich i danych dotyczących odmowy wjazdu w odniesieniu do obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich Unii Europejskiej oraz określające warunki dostępu do systemu wjazdu/wyjazdu na potrzeby ścigania i zmieniające rozporządzenie (WE) nr 767/2008 i rozporządzenie (UE) nr 1077/2011 (COM(2016) 194 final).

biometrycznych na potrzeby funkcjonowania systemu wjazdu/wyjazdu; w niniejszym wniosku starano się odzwierciedlić to podejście;

b) ETIAS, w ramach którego zaproponowano dokładną ocenę bezpieczeństwa, w tym kontrolę w SIS, przeprowadzaną w przypadku obywateli państw trzecich, którzy zamierzają podróżować na terytorium Unii Europejskiej i którzy są zwolnieni z obowiązku wizowego.

1.6. Okres trwania działania i jego wpływ finansowy

☐ Wniosek/inicjatywa o **ograniczonym okresie trwania**

– ☐ Okres trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

– ☐ Okres trwania wpływu finansowego: od RRRR r. do RRRR r.

☑ Wniosek/inicjatywa o **nieograniczonym okresie trwania**

– Wprowadzenie w życie z okresem rozruchu od 2018 r. do 2020 r.,

– po którym następuje faza operacyjna.

1.7. Przewidywane tryby zarządzania[88]

☑ **Bezpośrednie zarządzanie** przez Komisję

– ☑w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii;

– ☐ przez agencje wykonawcze

☑**Zarządzanie dzielone** z państwami członkowskimi

☑**Zarządzanie pośrednie** poprzez przekazanie zadań związanych z wykonaniem budżetu:

– ☐ państwom trzecim lub organom przez nie wyznaczonym;

– ☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

– ☐ EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

– ☑organom, o których mowa w art. 208 i 209 rozporządzenia finansowego;

– ☐ organom prawa publicznego;

– ☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile zapewniają one odpowiednie gwarancje finansowe;

– ☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego oraz które zapewniają odpowiednie gwarancje finansowe;

– ☐ osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym.

[88] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

– *W przypadku wskazania więcej niż jednego trybu należy podać dodatkowe informacje w części „Uwagi”.*

Uwagi

Komisja będzie odpowiedzialna za ogólne zarządzanie polityką, a eu-LISA będzie odpowiedzialna za opracowanie, działanie i utrzymanie systemu. **SIS stanowi jednolity system informacyjny. W związku z powyższym wydatki przewidziane w dwóch wnioskach (w niniejszym wniosku i we wniosku dotyczącym rozporządzenia w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych) należy uznać za jedną kwotę, a nie dwie oddzielne. Wpływ na budżet związany ze zmianami, których wymaga wdrożenie wniosków, ujęto w jednej ocenie skutków finansowych regulacji.**

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Należy określić częstotliwość i warunki.

Komisja, państwa członkowskie i Agencja będą prowadzić regularne przeglądy i monitorowanie użytkowania SIS, aby zapewnić jego skuteczne i wydajne funkcjonowanie. Komitet będzie pomagał Komisji we wdrażaniu środków technicznych i operacyjnych, jak przewidziano w niniejszym wniosku.

Ponadto niniejsze proponowane rozporządzenie zawiera przepisy (w art. 54 ust. 7 i 8) dotyczące przeprowadzania formalnego, regularnego procesu przeglądu i oceny.

Co dwa lata eu-LISA ma obowiązek przedkładać Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące technicznej sprawności – w tym bezpieczeństwa – SIS, infrastruktury łączności systemu oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi.

Ponadto co cztery lata Komisja ma obowiązek przeprowadzić i przekazać Parlamentowi i Radzie ogólną ocenę SIS i wymiany informacji między państwami członkowskimi. Umożliwi to:

a) analizę osiągniętych wyników w zestawieniu z celami;

b) określenie, na ile wciąż aktualne są pierwotne przesłanki systemu;

c) analizę sposobu, w jaki niniejsze rozporządzenie stosowane jest do systemu centralnego;

d) ocenę bezpieczeństwa systemu centralnego;

e) ocenę konsekwencji dla przyszłego funkcjonowania systemu.

2.2. Co więcej, obecnie eu-LISA powierzono również obowiązek dostarczania dziennych, miesięcznych i rocznych statystyk na temat sposobu wykorzystania SIS, co zapewnia stałe monitorowanie systemu i jego funkcjonowania w zestawieniu z celami.System zarządzania i kontroli

2.2.1. Zidentyfikowane ryzyko

Zidentyfikowano następujące zagrożenia.

1. Potencjalne problemy, jakie eu-LISA mogłaby napotkać w zarządzaniu zmianami przedstawionymi w niniejszym wniosku ze względu na inne obecnie wprowadzane zmiany (np. wprowadzenie automatycznego systemu identyfikacji daktyloskopijnej (AFIS) do SIS) oraz przyszłe zmiany (np. system wjazdu/wyjazdu, ETIAS i aktualizacja Eurodac). Zagrożenie to można ograniczyć poprzez zapewnienie eu-LISA takiej liczby pracowników i takich zasobów, które wystarczą do przeprowadzenia tych zadań, oraz bieżącego zarządzania systemem przez wykonawcę odpowiedzialnego za utrzymanie dobrego stanu technicznego systemu.

2. Trudności, jakie mogą napotkać państwa członkowskie

2.1 Trudności te mają przede wszystkim charakter finansowy. Przykładowo wnioski ustawodawcze wiążą się z obowiązkiem utworzenia częściowej kopii krajowej w każdym N.SIS II. Państwa członkowskie, które nie utworzyły takiej kopii, będą musiały liczyć się z wydatkami. Podobnie wprowadzenie dokumentu kontroli interfejsu na szczeblu krajowym powinno zostać przeprowadzone w sposób kompletny. Te państwa członkowskie, które jeszcze tego nie uczyniły, będą musiały uwzględnić ten wydatek w swoim budżecie odpowiednich ministerstw. Zagrożenie to można ograniczyć poprzez zapewnienie państwom członkowskim finansowania z UE, np. z Funduszu Bezpieczeństwa Wewnętrznego (element „Granice").

2.2 Systemy krajowe muszą odpowiadać centralnym wymogom, a dyskusje prowadzone w tym temacie z państwami członkowskimi mogą spowodować opóźnienia w osiągnięciu tego celu. Zagrożenie to można ograniczyć poprzez angażowanie państw członkowskich w tę kwestię już na wczesnym etapie, tak aby zagwarantować, że niezbędne działania zostaną podjęte w odpowiednim czasie.

2.2.2. Informacje dotyczące struktury wewnętrznego systemu kontroli

Za wypełnienie obowiązków związanych z głównymi elementami SIS odpowiada eu-LISA. Aby umożliwić lepsze monitorowanie wykorzystania SIS do celów analizy tendencji związanych z presją migracyjną, zarządzania granicami i przestępstwami, Agencja powinna mieć możliwość rozwijania nowoczesnych zdolności w zakresie prowadzenia sprawozdawczości statystycznej wobec państw członkowskich i Komisji.

Sprawozdanie finansowe eu-LISA podlega zatwierdzeniu przez Trybunał Obrachunkowy i procedurze udzielania absolutorium. Służba Audytu Wewnętrznego Komisji będzie przeprowadzać audyty we współpracy z audytorem wewnętrznym Agencji.

2.2.3. Oszacowanie kosztów i korzyści wynikających z kontroli i ocena prawdopodobnego ryzyka błędu

nie dotyczy

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony

Środki przewidziane na zwalczanie nadużyć finansowych zostały określone w art. 35 rozporządzenia (UE) nr 1077/2011, który stanowi następująco.

1. W celu zwalczania nadużyć finansowych, korupcji i innych bezprawnych działań zastosowanie ma rozporządzenie (WE) nr 1073/1999.

2. Agencja przystępuje do porozumienia międzyinstytucjonalnego dotyczącego wewnętrznych dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) i niezwłocznie wydaje odpowiednie przepisy, które mają zastosowanie do wszystkich pracowników Agencji.

3. Decyzje dotyczące finansowania oraz umowy i akty wykonawcze do nich powinny wyraźnie zastrzegać, że Trybunał Obrachunkowy i OLAF mogą, w razie konieczności, przeprowadzać kontrole na miejscu wśród odbiorców funduszy Agencji oraz urzędników odpowiedzialnych za ich przyznawanie.

Zgodnie z tym przepisem w dniu 28 czerwca 2012 r. przyjęto decyzję Zarządu Europejskiej Agencji do spraw Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości w sprawie zasad i warunków dochodzeń wewnętrznych w odniesieniu do przeciwdziałania nadużyciom finansowym, korupcji i wszelkim nielegalnym działaniom godzącym w interesy Unii.

Zastosowanie będzie miała strategia Dyrekcji Generalnej do Spraw Wewnętrznych dotycząca zapobiegania nadużyciom finansowym i ich wykrywania.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

- Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych.

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	[Dział 3 – Bezpieczeństwo i obywatelstwo	Zróżnicowane / niezróżnicowane[89]	państw EFTA[90]	krajów kandydujących[91]	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
	18.0208 System Informacyjny Schengen	Zróżnicowane	NIE	NIE	TAK	NIE
	18.020101 – Wsparcie zarządzania granicami oraz wspólnej polityki wizowej w celu ułatwienia legalnego podróżowania	Zróżnicowane	NIE	NIE	TAK	NIE
	18.0207 – Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA)	Zróżnicowane	NIE	NIE	TAK	NIE

89 Środki zróżnicowane / środki niezróżnicowane.

90 EFTA: Europejskie Stowarzyszenie Wolnego Handlu.

91 Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

Dział wieloletnich ram finansowych	3	Bezpieczeństwo i obywatelstwo

DG HOME			Rok **2018**	Rok **2019**	Rok **2020**	**OGÓŁEM**
• Środki operacyjne						
18.0208 System Informacyjny Schengen	Środki na zobowiązania	(1)	6,234	1,854	1,854	**9,942**
	Środki na płatności	(2)	6,234	1,854	1,854	**9,942**
18.020101 (Granice i wizy)	Środki na zobowiązania	(1)		18,405	18,405	**36,810**
	Środki na płatności	(2)		18,405	18,405	**36,810**
OGÓŁEM środki DG HOME	Środki na zobowiązania	=1+1a +3	6,234	20,259	20,259	**46,752**
	Środki na płatności	=2+2a +3	6,234	20,259	20,259	**46,752**

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	3	Bezpieczeństwo i obywatelstwo

eu-LISA			Rok **2018**	Rok **2019**	Rok **2020**	**OGÓŁEM**
• Środki operacyjne						
Tytuł 1: Wydatki na personel	Środki na zobowiązania	(1)	0,210	0,210	0,210	**0,630**
	Środki na płatności	(2)	0,210	0,210	0,210	**0,630**
Tytuł 2: Wydatki na infrastrukturę i wydatki administracyjne	Środki na zobowiązania	(1a)	0	0	0	**0**
	Środki na płatności	(2a)	0	0	0	**0**
Tytuł 3: Wydatki operacyjne	Środki na zobowiązania	(1a)	12,893	2,051	1,982	**16,926**
	Środki na płatności	(2a)	2,500	7,893	4,651	**15,044**
OGÓŁEM środki eu-LISA	Środki na zobowiązania	=1+1a +3	13,103	2,261	2,192	**17,556**
	Środki na	=2+2a	2,710	8,103	4,861	**15,674**

	płatności	+3				

3.2.2. Szacunkowy wpływ na środki operacyjne

• OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)								
	Środki na płatności	(5)								
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne		(6)								
OGÓŁEM środki na DZIAŁ <….> wieloletnich ram finansowych	Środki na zobowiązania	=4+ 6								
	Środki na płatności	=5+ 6								

Jeżeli wpływ wniosku/inicjatywy nie ogranicza się do jednego działu:

• OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)							
	Środki na płatności	(5)							
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne		(6)							
OGÓŁEM środki na DZIAŁY 1–4 wieloletnich ram finansowych (kwota referencyjna)	Środki na zobowiązania	=4+ 6	19,337	22,520	22,451				**64,308**
	Środki na płatności	=5+ 6	8,944	28,362	25,120				**62,426**

3.2.3. Szacunkowy wpływ na środki administracyjne

Dział wieloletnich ram finansowych	**5**	„Wydatki administracyjne”

w mln EUR (do trzech miejsc po przecinku)

		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			**OGÓŁEM**
Dyrekcja Generalna: <…….>									
• Zasoby ludzkie									
• Pozostałe wydatki administracyjne									
OGÓŁEM Dyrekcja Generalna <…….>	Środki								

OGÓŁEM środki na DZIAŁ 5 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)								

w mln EUR (do trzech miejsc po przecinku)

		Rok **N**[92]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			**OGÓŁEM**
OGÓŁEM środki	Środki na zobowiązania								

[92] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy.

na DZIAŁY 1–5 wieloletnich ram finansowych	Środki na płatności								

3.2.3.1. Szacunkowy wpływ na środki operacyjne eu-LISA

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Określić cele i produkty			Rok **2018**		Rok **2019**		Rok **2020**		Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)						**OGÓŁEM**			
	PRODUKT																	
⇩	Rodzaj[93]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY nr 1[94] Rozwój systemu centralnego																		
- Wykonawca			1	5,013														5,013
-			1	4,050														4,050
- Sprzęt			1	3,692														3,692
Cel szczegółowy nr 1 – suma cząstkowa				12,755														12,755
CEL SZCZEGÓŁOWY nr 2 Konserwacja systemu centralnego																		
- Wykonawca			1	0	1	0,365	1	0,365										0,730
Oprogramowani			1	0	1	0,810	1	0,810										1,620
Sprzęt			1	0	1	0,738	1	0,738										1,476

[93] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[94] Zgodnie z opisem w pkt 1.4.2. „Cel(-e) szczegółowy(-e)…”.

Cel szczegółowy nr 2 – suma cząstkowa				1,913		1,913										3,826
CEL SZCZEGÓŁOWY nr 3 Spotkania/szkolenia																
Działania szkoleniowe	1	0,138	1	0,138	1	0,069										0,345
Cel szczegółowy nr 3 – suma cząstkowa		0,138		0,138		0,069										0,345
KOSZT OGÓŁEM		12,893		2,051		1,982										16,926

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

3.2.3.2. Szacunkowy wpływ na środki DG HOME

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Określić cele i produkty			Rok **2018**		Rok **2019**		Rok **2020**		Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)						**OGÓŁEM**			
	PRODUKT																	
⇩	Rodzaj[95]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY nr 1[96] Rozwój systemu krajowego			1		1	1,221	1	1,221										2,442

[95] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[96] Zgodnie z opisem w pkt 1.4.2. „Cel(-e) szczegółowy(-e)…”.

CEL SZCZEGÓŁOWY nr 2 Infrastruktura	1		1	17,184	1	17,184										34,368
KOSZT OGÓŁEM				18,405		18,405										36,810

3.2.3.3. Szacunkowy wpływ na zasoby ludzkie eu-LISA – zestawienie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok **2018**	Rok **2019**	Rok **2020**	**OGÓŁEM**
Urzędnicy (grupa zaszeregowania AD)				
Urzędnicy (grupa zaszeregowania AST)				
Personel kontraktowy	0,210	0,210	0,210	0,630
Pracownicy zatrudnieni na czas określony				
Oddelegowani eksperci krajowi				
OGÓŁEM	**0,210**	**0,210**	**0,210**	**0,630**

Rekrutację zaplanowano na styczeń 2018 r. Wszyscy pracownicy muszą być dostępni już na początku 2018 r., tak aby faza rozwojowa mogła rozpocząć się w odpowiednim czasie, zapewniając tym samym uruchomienie SIS II (wersja przekształcona) w 2020 r. W celu zaspokojenia potrzeb zarówno w zakresie wdrażania projektu, jak i wsparcia operacyjnego i konserwacji po rozmieszczeniu do produkcji potrzebni są trzej nowi pracownicy kontraktowi. Pracownicy ci będą:

- wspierać wdrażanie projektu jako członkowie zespołu projektowego, podejmując działania takie jak: określenie wymogów i specyfikacji technicznych, współpraca i wspieranie państw członkowskich w trakcie wdrażania, aktualizacje dokumentu kontroli interfejsu (ICD), działania następcze w związku z dostarczaniem usług na podstawie umowy, dostarczaniem i aktualizacją dokumentacji itp.;

- wspierać działania przejściowe związane z uruchomieniem systemu we współpracy z wykonawcą (działania następcze, operacyjne aktualizacje procesowe, szkolenia (w tym działania szkoleniowe państw członkowskich) itp.);

- wspierać działania długofalowe, określanie specyfikacji, przygotowania podejmowane na podstawie umowy w przypadku przeprogramowania systemu (np. ze względu na rozpoznawanie wizerunku) lub w przypadku, gdy umowa dotycząca utrzymania dobrego stanu technicznego nowego SIS II będzie

wymagała modyfikacji ze względu na dodatkowe zmiany (z perspektywy technicznej i budżetowej);

- wzmacniać wsparcie drugiego szczebla po uruchomieniu systemu w trakcie ciągłej konserwacji i działania systemu.

Należy podkreślić, że trzej nowi pracownicy (EPC CA) będą działać obok wewnętrznych zespołów, które również będą podejmować działania związane z projektem/umową oraz finansowe działania następcze i działania operacyjne. Dzięki nowym pracownikom umowy będą obowiązywać przez odpowiedni czas i zagwarantuje to ich ciągłość w celu zapewnienia ciągłości działania i wykorzystywania usług tych samych specjalistów w działaniach o charakterze wsparcia operacyjnego po zakończeniu projektu. Ponadto wsparcie operacyjne wymaga dostępu do środowiska produkcyjnego, którego nie można udzielić wykonawcom ani pracownikom zewnętrznym.

3.2.3.4. Szacowane zapotrzebowanie na zasoby ludzkie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich

– ☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy

		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)		
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)								
XX 01 01 01 (w centrali i w biurach przedstawicielstw Komisji)								
XX 01 01 02 (w delegaturach)								
XX 01 05 01 (pośrednie badania naukowe)								
10 01 05 01 (bezpośrednie badania naukowe)								
• Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC)[97]								
XX 01 02 01 (CA, SNE, INT z globalnej koperty finansowej)								
XX 01 02 02 (CA, LA, SNE, INT i JED w delegaturach)								
XX 01 04 **yy** [98]	- w centrali							
	- w delegaturach							
XX 01 05 02 (CA, SNE, INT – pośrednie badania naukowe)								
10 01 05 02 (CA, SNE, INT – bezpośrednie badania naukowe)								
Inna linia budżetowa (określić)								
OGÓŁEM								

XX oznacza odpowiednią dziedzinę polityki lub odpowiedni tytuł w budżecie

97 CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JED = młodszy oddelegowany ekspert.

98 W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA").

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	
Personel zewnętrzny	

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

– ☐ Wniosek/inicjatywa jest zgodny(-a) z obowiązującymi wieloletnimi ramami finansowymi.

– ☑ Wniosek/inicjatywa wymaga przeprogramowania odpowiedniego działu w wieloletnich ramach finansowych.

W celu wdrożenia funkcji i zmian przewidzianych w przedmiotowych dwóch wnioskach zaplanowano przeprogramowanie pozostałej części puli środków przeznaczonych w ramach Funduszu Bezpieczeństwa Wewnętrznego na inicjatywę na rzecz inteligentnych granic. Rozporządzenie w sprawie Funduszu Bezpieczeństwa Wewnętrznego i wsparcia w zakresie granic jest instrumentem finansowym, w którym uwzględniono budżet przeznaczony na realizację pakietu dotyczącego inteligentnych granic. W art. 5 przewidziano, że kwota 791 mln EUR zostanie wykorzystana za pośrednictwem programu tworzenia nowych systemów informatycznych wspierających zarządzanie przepływami migracyjnymi przez granice zewnętrzne Unii, na warunkach ustanowionych w art. 15. Z podanej powyżej kwoty 791 mln EUR kwota 480 mln EUR jest zarezerwowana na rozwój systemu wjazdu/wyjazdu, a kwota 210 mln EUR – na rozwój europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS). Część pozostałej kwoty w wysokości 100 828 mln EUR zostanie przeznaczona na pokrycie kosztów zmian przewidzianych w przedmiotowych dwóch wnioskach.

– ☐ Wniosek/inicjatywa wymaga zastosowania instrumentu elastyczności lub zmiany wieloletnich ram finansowych.

Należy wyjaśnić, który wariant jest konieczny, określając linie budżetowe, których ma on dotyczyć, oraz podając odpowiednie kwoty.

3.2.5. Udział osób trzecich w finansowaniu

– ☑ Wniosek/inicjatywa nie przewiduje współfinansowania ze strony osób trzecich

– Wniosek/inicjatywa przewiduje współfinansowanie szacowane zgodnie z poniższym:

Środki w mln EUR (do trzech miejsc po przecinku)

	Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			Ogółem
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

3.3. Szacunkowy wpływ na dochody

– ☐ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

– ☑ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

– ☐ wpływ na zasoby własne

– ☑ wpływ na dochody różne

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[99]						
		2018	2019	2020	2021	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)		
Artykuł 6313 – wkład państw stowarzyszonych w ramach Schengen (CH, NO, LI, IS).		p.m.	p.m.	p.m.	p.m.			

W przypadku wpływu na dochody różne „przeznaczone na określony cel” należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

18.02.08 (System Informacyjny Schengen), 18.02.07 (eu-LISA)

Należy określić metodę obliczania wpływu na dochody.

Budżet obejmuje wkład państw stowarzyszonych we wdrażaniu, stosowaniu i rozwijaniu dorobku Schengen.

[99] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 25 % na poczet kosztów poboru.