



KOMISJA
EUROPEJSKA

Bruksela, dnia 21.12.2016 r.
COM(2016) 883 final

2016/0409 (COD)

Wniosek

ROZPORZĄDZENIE 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, zmieniające rozporządzenie (UE) nr 515/2014 i uchylające rozporządzenie (WE) nr 1986/2006, decyzję Rady 2007/533/WSiSW i decyzję Komisji 2010/261/UE

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

W swoich pracach prowadzonych na przestrzeni ostatnich dwóch lat Unia Europejska mierzyła się jednocześnie z odrębnymi wyzwaniem 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 ocenę¹ 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 następnych 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 podstawę prawną utworzenia, funkcjonowania i użytkowania SIS. Wniosek dotyczący

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. ...).

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/WE².

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 wniosków⁴. 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 1077/2011⁵ 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).

Niniejszy wniosek stanowi element pierwszego zestawu wniosków⁶ służących poprawie funkcjonowania SIS oraz jego działania i użytkowania w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych. W niniejszym wniosku:

- 1) wdraża się oświadczenie Komisji zapowiadające zwiększenie wartości dodanej SIS na potrzeby ścigania przestępstw⁷ do celów reagowania na nowe zagrożenia;
- 2) 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;
- 3) wdraża się zalecenia dotyczące wprowadzenia technicznych i proceduralnych zmian w następstwie kompleksowej oceny SIS⁸;
- 4) wdraża się usprawnienia techniczne, o które wnioskowali użytkownicy końcowi SIS; oraz
- 5) wprowadza się wstępne ustalenia dotyczące jakości danych sformułowane przez grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności⁹.

Ponieważ przedmiotowy wniosek jest nierozdzielnie powiązany z wnioskiem Komisji dotyczącym rozporządzenia w sprawie utworzenia, funkcjonowania i użytkowania SIS w dziedzinie odpraw granicznych, 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 biometrycznych¹⁰.

Obowiązujące obecnie ramy prawne SIS drugiej generacji – w zakresie użytkowania systemu do celów współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych – opierają się na wcześniejszym instrumencie trzeciego filaru, tj. decyzji Rady 2007/533/WSiSW¹¹, oraz na wcześniejszym instrumencie pierwszego filaru, tj. rozporządzeniu Rady (WE) nr 1986/2006¹². W niniejszym wniosku ujednolicią się treści istniejących instrumentów i jednocześnie dodaje się nowe przepisy w celu:

⁶ Rozporządzenie (UE) 2018/xxx [odprawa graniczna] i rozporządzenie (UE) 2018/xxx [powrót nielegalnie przebywających obywateli państw trzecich].

⁷ Zob. komunikat „Realizacja Europejskiej agendy bezpieczeństwa w celu zwalczania terroryzmu i utorowania drogi ku rzeczywistej i skutecznej unii bezpieczeństwa”, s. 4f, COM(2016) 230 final z 20.4.2016.

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. ...).

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 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).

¹² Rozporządzenie (WE) nr 1986/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie dostępu służb odpowiedzialnych w państwach członkowskich za wydawanie świadectw

- zapewnienia lepszej harmonizacji procedur krajowych na potrzeby użytkowania SIS, w szczególności w odniesieniu do przestępstw związanych z terroryzmem oraz dzieci, w przypadku których istnieje ryzyko, że zostaną uprowadzone przez jednego z rodziców;
 - rozszerzenia zakresu stosowania SIS poprzez wprowadzenie nowych elementów identyfikatorów biometrycznych do istniejących wpisów;
 - wprowadzenia zmian technicznych w celu zwiększenia bezpieczeństwa i ograniczenia obciążenia administracyjnego poprzez wprowadzenie obowiązkowych kopii krajowych i wspólnych standardów technicznych do celów wdrożenia;
 - uwzględnienia pełnego użytkowania całego SIS, w tym nie tylko samego funkcjonowania systemu centralnego i systemu krajowego, lecz także zapewnienia, aby użytkownicy końcowi otrzymywali wszystkie dane, które są im niezbędne do wykonywania powierzonych im zadań, oraz aby przestrzegali oni wszystkich zasad bezpieczeństwa podczas przetwarzania danych SIS.
- **Spójność z innymi obszarami polityki Unii oraz z obowiązującymi i przyszłymi instrumentami prawnymi**

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

- 1) **bezpieczeństwo wewnętrzne**, jak podkreślono w Europejskiej agencji bezpieczeństwa¹³ oraz w ramach prac Komisji nad skuteczną i rzeczywistą unią bezpieczeństwa¹⁴, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, wykrywania ich, prowadzenia dochodzeń w ich sprawach i ścigania ich poprzez umożliwienie organom ścigania przetwarzania danych osobowych osób podejrzanych o udział w aktach terrorystycznych lub w poważnych przestępstwach;
- 2) **ochrona danych** w zakresie, w jakim w niniejszym wniosku zapewnia się ochronę praw podstawowych osób, których dane osobowe są przetwarzane w SIS.

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

- 3) przepisy dotyczące **Europejskiej Straży Granicznej i Przybrzeżnej** w zakresie jej dostępu do SIS do celów proponowanego europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS)¹⁵, a także w celu zapewnienia interfejsu technicznego zapewniającego dostęp do SIS europejskim zespołom straży granicznej, zespołom składającym się z personelu realizującego zadania w dziedzinie powrotów oraz członkom zespołu wspierającego zarządzanie migracjami, aby osoby te miały prawo, w granicach powierzonych im uprawnień, do uzyskania dostępu do danych wprowadzanych do SIS oraz do wyszukiwania tego rodzaju danych;

rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 381 z 28.12.2006, s. 1).

¹³ COM(2015) 185 final.

¹⁴ COM(2016) 230 final.

¹⁵ COM(2016) 731 final.

- 4 przepisy dotyczące **Europolu** w zakresie, w jakim w niniejszym wniosku Europolowi udziela się dodatkowych praw, w granicach jego uprawnień, do dostępu do danych wprowadzanych do SIS i do wyszukiwania tego rodzaju danych;
- 5) ramy z **Prüm** w zakresie, w jakim zmiany wprowadzone niniejszym wnioskiem w celu umożliwienia identyfikacji osób fizycznych na podstawie odcisków palców (jak i wizerunków twarzy i profili DNA) uzupełniają obowiązujące ramy z Prüm¹⁶ dotyczące wzajemnego transgranicznego dostępu online do wyznaczonych krajowych baz danych DNA i systemów automatycznej identyfikacji daktyloskopijnej.

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

- 6) przepisy dotyczące **zarządzania granicami zewnętrznymi**. Niniejszy wniosek uzupełnia przewidywaną nową zasadę kodeksu granicznego Schengen dotyczącą systematycznych kontroli wszystkich podróżnych, w tym obywateli Unii, w odpowiednich bazach danych w momencie wjazdu do strefy Schengen i jej opuszczania, które to kontrole mają zostać wprowadzone w odpowiedzi na działalność zagranicznych bojowników terrorystycznych;
- 7) **przepisy dotyczące systemu wjazdu/wyjazdu**. Wniosek ma uwzględniać proponowane wykorzystanie połączenia odcisków palców i wizerunku twarzy jako identyfikatorów biometrycznych na potrzeby funkcjonowania systemu wjazdu/wyjazdu;
- 8) **przepisy dotyczące ETIAS**. We wniosku uwzględnia się proponowany system ETIAS, w ramach którego przewiduje się dokładną ocenę bezpieczeństwa, w tym kontrolę w SIS, przeprowadzaną w przypadku obywateli państw trzecich, którzy zamierzają podróżować na terytorium UE.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawę prawną dla przepisów niniejszego wniosku dotyczących współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych stanowią art. 82 ust. 1 lit. d), art. 85 ust. 1, art. 87 ust. 2 lit. a) i art. 88 ust. 2 lit. a) Traktatu o Funkcjonowaniu Unii Europejskiej.

• Zmienna geometria

Niniejszy wniosek opiera się na dorobku Schengen związanym ze współpracą policyjną i współpracą wymiarów sprawiedliwości w sprawach karnych. 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

¹⁶ Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.U. L 210 z 6.8.2008, s. 1), oraz decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. w sprawie wdrożenia decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.U. L 210 z 6.8.2008, s. 12).

decyzji w sprawie niniejszego rozporządzenia, czy dokona transpozycji niniejszego wniosku, stanowiącego rozwinięcie dorobku Schengen, do swojego prawa krajowego.

Zjednoczone Królestwo: Zjednoczone Królestwo jest związane niniejszym rozporządzeniem zgodnie z art. 5 Protokołu w sprawie dorobku Schengen włączonego w ramy Unii Europejskiej, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, oraz art. 8 ust. 2 decyzji Rady 2000/365/WE z dnia 29 maja 2000 r. dotyczącej wniosku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o zastosowaniu wobec niego niektórych przepisów dorobku Schengen¹⁷.

Irlandia: Irlandia jest związana niniejszym rozporządzeniem zgodnie z art. 5 Protokołu w sprawie dorobku Schengen włączonego w ramy Unii Europejskiej, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, oraz art. 6 ust. 2 decyzji Rady 2002/192/WE z dnia 28 lutego 2002 r. dotyczącej wniosku Irlandii o zastosowanie wobec niej niektórych przepisów dorobku Schengen¹⁸.

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.¹⁹, 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.

• **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 za pośrednictwem SIS 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.

¹⁷ Dz.U. L 131 z 1.6.2000, s. 43.

¹⁸ Dz.U. L 64 z 7.3.2002, s. 20.

¹⁹ 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).

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 współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych.

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. Uwzględniając wymogi operacyjne, w niniejszym wniosku ogranicza się okres przechowywania wpisów dotyczących przedmiotów i ujednolica się go z okresem przechowywania wpisów dotyczących osób (ponieważ wielokrotnie tego rodzaju wpisy wiążą się z danymi osobowymi, jak w przypadku dokumentów tożsamości lub tablic rejestracyjnych). Jako że z doświadczeń policji wynika, że skradzione mienie można odzyskać w stosunkowo krótkim czasie, nie ma potrzeby przechowywania wpisów dotyczących przedmiotów przez okres 10 lat.

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 zostanie przeprowadzona w drodze rozporządzenia, które zastąpi decyzję Rady 2007/533/WSiSW, zachowując jednak w dużym stopniu treść zastępowanej decyzji. 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 konieczne, 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 Sprawiedliwości²⁰ (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.

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 trzy lata po rozpoczęciu eksploatacji centralnego SIS II Komisja przeprowadziła ogólną ocenę centralnego SIS II oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi.

Wyniki oceny uwiaryściły konieczność wprowadzenia zmian do podstawy prawnej SIS w celu zapewnienia lepszego reagowania na nowe wyzwania w zakresie bezpieczeństwa i migracji. Dotyczy to na przykład wniosku w sprawie całościowego stosowania SIS poprzez uregulowanie jego użytkowania przez użytkowników końcowych i ustanowienie standardów w zakresie bezpieczeństwa danych obowiązujących również w przypadku zastosowań przez użytkowników końcowych, w sprawie wzmocnienia systemu do celów zwalczania terroryzmu poprzez zapewnienie nowych niezbędnych do podjęcia działań, w sprawie wyjaśnienia sytuacji dzieci zagrożonych uprowadzeniem przez rodziców, a także w sprawie rozszerzenia bazy identyfikatorów biometrycznych dostępnych w systemie.

W wyniku wspomnianej oceny wykazano również potrzebę zmian prawnych mających na celu poprawę technicznego funkcjonowania systemu oraz usprawnienia procesów krajowych.

²⁰ 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).

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 przyjęte w dniu 21 grudnia 2016 r.²¹) stanowią podstawę środków zawartych w niniejszym wniosku.

- **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. 67 decyzji Rady 2007/533/WSiSW, 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.

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

²¹ 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.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

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

- Ocena techniczna SIS (Kurt Salmon)²²

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)²³

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)²⁴

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).

- **Ocena skutków**

Komisja nie przeprowadziła oceny skutków.

Trzy wyżej wymienione niezależne oceny (w sekcji „Gromadzenie i wykorzystanie wiedzy eksperckiej”) stanowią podstawę rozważań na temat skutków zmian w systemie z technicznego punktu widzenia. Ponadto Komisja przeprowadziła dwa 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 śródkresowy, w wyniku którego w dniu 29 stycznia 2015 r. wprowadzono nowy podręcznik SIRENE²⁵. Komisja przyjęła również Katalog zaleceń i najlepszych praktyk²⁶.

²² SPRAWOZDANIE KOŃCOWE Komisji Europejskiej – Ocena techniczna SIS II.

²³ SPRAWOZDANIE KOŃCOWE Komisji Europejskiej – Ocena wpływu technologii informacyjno-komunikacyjnych na potencjalne usprawnienia w architekturze SIS II z 2016 r.

²⁴ SPRAWOZDANIE KOŃCOWE Komisji Europejskiej – Ocena wpływu technologii informacyjno-komunikacyjnych na potencjalne usprawnienia w architekturze SIS II – sprawozdanie końcowe, 10 listopada 2016 r., (Wavestone)

²⁵ 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).

²⁶ Zalecenie Komisji w sprawie ustanowienia Katalogu zaleceń i najlepszych praktyk dotyczących właściwego stosowania systemu informacyjnego Schengen (SIS II) oraz wymiany informacji

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 1053/2013²⁷, 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 zaginionych małoletnich dzieci. 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.

uzupełniających przez właściwe organy państw członkowskich wdrażające i wykorzystujące SIS II [C(2015)9169/1].

²⁷ 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 uchylecia 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).

- **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 konieczne 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 ustanawia się wyraźne ramy czasowe dotyczące przechowywania danych, w tym ograniczone okresy przechowywania wpisów dotyczących przedmiotów. 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. Bardziej wiarygodna identyfikacja osób fizycznych będzie możliwa za sprawą wykorzystania danych biometrycznych w odniesieniu do osób zaginionych, które wymagają ochrony dzięki zapewnieniu prawidłowości i odpowiedniej ochrony danych osobowych. 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 Europejskiej²⁸ 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. 26, 32, 34 i 36. 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 aktu terrorystycznego, oraz jeżeli z dużym prawdopodobieństwem można stwierdzić, że znalezione ślady linii papilarnych należą do sprawcy. W niniejszym wniosku przewidziano ponadto przechowywanie obrazu linii papilarnych tak zwanych „nieznanych osób poszukiwanych” (szczegółowy opis warunków znajduje się w sekcji 5 podsekcja „Fotografie, wizerunki twarzy, dane daktyloskopijne i profile DNA”). Jeżeli na podstawie dokumentów danej osoby nie można z całą pewnością ustalić jej tożsamości, właściwe organy powinny sprawdzić, czy jej odciski palców można dopasować do odcisków palców przechowywanych w bazie danych SIS.

²⁸

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

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. WPLYW 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 odpraw granicznych) 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 wniosek²⁹. 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

²⁹ 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.

środków przeznaczonych w ramach Funduszu Bezpieczeństwa Wewnętrznego na inicjatywę na rzecz inteligentnych granic. Rozporządzenie w sprawie Funduszu Bezpieczeństwa Wewnętrznego i wsparcia w zakresie granic³⁰ 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 podróżach 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 przepisy w art. 71 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 oraz przekazać Parlamentowi i Radzie ogólną ocenę SIS i wymiany informacji między państwami członkowskimi. Umożliwi to:

- 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.

³⁰

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).

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Przepisy wspólne dla niniejszego wniosku i wniosku dotyczącego rozporządzenia w sprawie utworzenia, funkcjonowania i użytkowania SIS w dziedzinie odpraw granicznych

- 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. 43, 46, 48, 50 i 51)
- Ogólne zasady przetwarzania i ochrony danych (art. 53–70)
- Monitorowanie i statystyka (art. 71)

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) 2016/680³¹.

³¹ 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

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. 56). 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. 71). 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. Ponadto dzięki zmianom w art. 22 oraz wprowadzeniu nowych art. 40, 41 i 42 tożsamość danej osoby będzie można ustalić nie tylko za pomocą odcisków palców, ale także wizerunków twarzy, odcisków dłoni i profili DNA. Obecnie wizerunków twarzy nie można wykorzystywać jako podstawowego kryterium wyszukiwania – mogą one być wykorzystywane wyłącznie w celu potwierdzenia tożsamości danej osoby po przeprowadzeniu wyszukiwania alfanumerycznego. 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. Odciski dłoni mają dwa główne zastosowania:

- i) 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 system automatycznej identyfikacji daktyloskopijnej (AFIS) we Włoszech odnotował istotny sukces pod względem identyfikacji nielegalnych migrantów, którzy celowo niszczyli swoje opuszki palców, usiłując uniknąć identyfikacji. Pobranie odcisków dłoni umożliwiło władzom włoskim późniejszą identyfikację;

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).

- ii) niewidoczne ślady linii papilarnych na miejscach przestępstwa. Na miejscu przestępstwa podejrzany często zostawia ślady, co do których okazuje się, że pochodzą z dłoni. W takiej sytuacji podejrzany może zostać zidentyfikowany wyłącznie dzięki rutynowemu pobieraniu odcisków dłoni przy okazji zgodnego z prawem pobrania odcisków palców danej osoby. Zazwyczaj odcisk dłoni zawiera szczegółowy odcisk podstawy palców, którego często brakuje przy pobieraniu odbitek przetoczonych i płaskich, w przypadku których główną uwagę przykładą się do pobrania odcisków opuszków palców i górnych stawów.

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.

Jeżeli odciski palców lub odciski dłoni są niedostępne, w art. 22 ust. 1 lit. b) dopuszcza się wykorzystanie profili DNA w przypadku osób zaginionych, które należy objąć ochroną, szczególnie dzieci. Funkcja ta będzie wykorzystywana wyłącznie w przypadku braku odcisków palców, a dostęp do niej będą mieli wyłącznie upoważnieni użytkownicy. W ramach przedmiotowego przepisu dopuszcza się zatem wykorzystanie profili DNA za pośrednictwem rodziców lub rodzeństwa zaginionych osób/dzieci do celów ułatwienia organom krajowym identyfikacji danej osoby fizycznej. Państwa członkowskie wymieniają się już tego rodzaju informacjami na poziomie operacyjnym w ramach wymiany informacji uzupełniających. Niniejszy wniosek tworzy ramy regulacyjne dla tej praktyki poprzez włączenie jej do merytorycznej podstawy prawnej funkcjonowania i użytkowania SIS oraz poprzez wdrożenie wyraźnych procesów stosowanych w przypadku wystąpienia okoliczności, w których możliwe jest zastosowanie tego rodzaju profili.

Proponowane zmiany umożliwią ponadto dokonywanie wpisów w SIS dotyczących osób nieznanych poszukiwanych w związku z przestępstwem na podstawie odcisków palców lub odcisków dłoni (art. 40–42). Tego rodzaju wpisy można tworzyć, jeżeli na przykład na miejscu poważnego przestępstwa zostaną odkryte niewidoczne ślady linii papilarnych lub odcisków dłoni i istnieją poważne powody, aby podejrzewać, że znalezione ślady linii papilarnych należą do sprawcy danego przestępstwa. Dotyczy to na przykład śladów linii papilarnych znalezionych na broni wykorzystanej do popełnienia przestępstwa lub na dowolnym innym przedmiocie, którym posługiwał się sprawca w czasie popełnienia przestępstwa. Ta nowa kategoria wpisów stanowi uzupełnienie przepisów dotyczących mechanizmu Prüm, w których umożliwiono wzajemne połączenie krajowych systemów identyfikacji daktyloskopijnej w sprawach karnych. Za pomocą mechanizmu Prüm państwo członkowskie może wystąpić z wnioskiem o ustalenie, czy sprawca przestępstwa, którego ślady linii papilarnych zostały znalezione, jest znany w innym państwie członkowskim (zazwyczaj do celów śledczych). Identyfikacja danej osoby za pomocą mechanizmu Prüm jest możliwa wyłącznie w przypadku, gdy od danej osoby pobrano odciski palców w innym państwie członkowskim na potrzeby postępowania karnego. W ten sposób nie można zatem zidentyfikować osób popełniających przestępstwo po raz pierwszy. Zmiany wprowadzane w niniejszym wniosku, tzn. przechowywanie obrazu linii papilarnych nieznanych osób poszukiwanych, umożliwią wprowadzenie linii papilarnych nieznanego sprawcy do SIS, aby – w momencie gdy pojawi się on w innym państwie członkowskim – został zidentyfikowany jako osoba poszukiwana. Funkcję tę stosuje się w oparciu o założenie, że państwa członkowskie w pierwszej kolejności przeszukały wszystkie dostępne źródła krajowe i międzynarodowe, lecz nie mogły w ten sposób potwierdzić tożsamości danej osoby. Niniejszy wniosek zawiera wystarczające zabezpieczenia gwarantujące, że w tej kategorii w SIS będą przechowywane obrazy linii papilarnych wyłącznie osób, co do których istnieje poważne

podejrzanie, że popełniły poważne przestępstwo lub przestępstwo terrorystyczne. W związku z tym stosowanie tej nowej kategorii wpisów może być dozwolone wyłącznie w przypadku, gdy nieznaną sprawcą stanowi duże zagrożenie dla bezpieczeństwa publicznego uzasadniające porównanie jego linii papilarnych z odciskami palców podróźnych, przykładowo aby uniknąć sytuacji, w której dana osoba opuści obszar bez kontroli na granicach wewnętrznych.

W przedmiotowym przepisie nie dopuszcza się możliwości wprowadzania odcisków palców w tej kategorii przez użytkowników końcowych, jeżeli nie jest możliwe ustalenie ich związku ze sprawcą. Kolejnym warunkiem będzie brak możliwości ustalenia tożsamości danej osoby za pomocą innych krajowych, europejskich lub międzynarodowych baz danych, w których przechowywane są odciski palców. Tego rodzaju linie papilarne będzie można wykorzystać po ich umieszczeniu w SIS do celów identyfikacji osób, których tożsamości nie można potwierdzić w żaden inny sposób. Jeżeli wyszukiwane linie papilarne pokryją się z odciskami dostępnymi w bazie danych, państwo członkowskie powinno przeprowadzić dalsze kontrole dotyczące posiadanych odcisków palców, ewentualnie z udziałem ekspertów daktyloskopijnych w celu ustalenia, czy odciski przechowywane w SIS należą do danej osoby, oraz powinno ustalić tożsamość danej osoby. Tego rodzaju procedury podlegają prawu krajowemu. Identyfikacja „nieznanej osoby poszukiwanej” w SIS może doprowadzić do aresztowania.

Dostęp do SIS

Niniejsza podsekcja zawiera opis nowych elementów dotyczących praw dostępu do SIS w odniesieniu do właściwych organów krajowych oraz agencji UE (użytkownicy instytucjonalni).

Organy krajowe – organy ds. imigracji

Aby zapewnić jak najskuteczniejsze wykorzystanie SIS, we wniosku udziela się dostępu do SIS organom krajowym odpowiedzialnym za badanie warunków i podejmowanie decyzji w związku z wjazdem i pobytem obywateli państw trzecich na terytorium państw członkowskich oraz ich powrotem. Ten dodatkowy dostęp umożliwia sprawdzenie danych w SIS w odniesieniu do nielegalnych migrantów, którzy nie zostali sprawdzeni podczas zwykłej kontroli granicznej. W niniejszym wniosku zapewnia się takie samo traktowanie obywateli państw trzecich przekraczających granicę zewnętrzną przez zwykłe przejścia graniczne (i tym samym poddawanych kontrolom stosowanym wobec obywateli państw trzecich) i obywateli państw trzecich przybywających nielegalnie do strefy Schengen.

W niniejszym wniosku zapewnia się ponadto, aby organy rejestrujące pojazdy (art. 44), jednostki pływające i statki powietrzne miały ograniczony dostęp do systemu do celów wykonania swoich zadań, pod warunkiem że tego rodzaju organy są służbami rządowymi. Przyczyni się to do unikania sytuacji, w których zarejestrowane zostają wymienione środki transportu, które zostały skradzione i są poszukiwane w innych państwach członkowskich. Niniejsza inicjatywa nie stanowi nowości, jeżeli chodzi o służby rejestrujące pojazdy, których dostęp do SIS przewidziano już w art. 102a konwencji z Schengen oraz w rozporządzeniu (WE) nr 1986/2006³². Analogicznie we wniosku przewidziano dostęp organów rejestrujących jednostki pływające i statki powietrzne do wpisów w SIS dotyczących jednostek pływających i statków powietrznych.

³² Rozporządzenie (WE) nr 1986/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie dostępu służb odpowiedzialnych w państwach członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 381 z 28.12.2006, s. 1).

Użytkownicy instytucjonalni

Dostęp do SIS i potrzebnych danych w SIS mają: Europol (art. 46), Eurojust (art. 47) 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 (art. 48 i 49). Wprowadza się odpowiednie zabezpieczenia w celu zapewnienia, aby dane w systemie były odpowiednio chronione (czemu służą również przepisy art. 50, 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 osób zaginionych, 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. W kontekście prac grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności oraz w celu wzmocnienia wymiany informacji w dziedzinie terroryzmu Komisja zbada, czy Europol powinien automatycznie dostawać powiadomienie z SIS w momencie utworzenia wpisu dotyczącego działalności związanej z terroryzmem.

Ponadto na podstawie wniosku Komisji dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)³³ jednostka centralna ETIAS Europejskiej Agencji Straży Granicznej i Przybrzeżnej będzie wyszukiwać dane w SIS za pomocą ETIAS, aby stwierdzić, 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 pełny dostęp do SIS.

Szczegółowe zmiany dotyczące wpisów

Artykuł 26 przewiduje możliwość tymczasowego zawieszenia przez państwa członkowskie wpisów mających doprowadzić do aresztowania (w przypadku tocących się operacji lub dochodzeń policji), tak aby przez określony czas tego rodzaju wpisy były widoczne wyłącznie dla biur SIRENE, ale nie dla funkcjonariuszy w terenie. Przepis ten służy uniknięciu sytuacji, w której powodzenie tajnej operacji policji mającej na celu aresztowanie groźnego poszukiwanego przestępcy zostaje zagrożone przez działanie funkcjonariusza policji niebiorącego udziału w danej sprawie.

W art. 32 i 33 ustanawia się wpisy dotyczące osób zaginionych. W ramach zmian w przedmiotowych przepisach przewiduje się możliwość wprowadzania wpisów prewencyjnych w sytuacjach, w których ryzyko uprowadzenia dziecka przez jednego z rodziców uznaje się za wysokie, a także ustanawia się bardziej adekwatną kategoryzację wpisów dotyczących osób zaginionych. Uprowadzenie dziecka przez jednego z rodziców często odbywa się w dokładnie zaplanowanych okolicznościach z zamiarem szybkiego opuszczenia państwa członkowskiego, w których dokonano ustaleń dotyczących pieczy. W ramach przedmiotowych zmian rozwiązuje się kwestię potencjalnej luki w obowiązujących obecnie przepisach, na podstawie których wpisy dotyczące dzieci można wprowadzać dopiero po ich zaginięciu. Dzięki zmianie w przepisach władze w państwach członkowskich będą mogły wskazywać dzieci, w

³³

COM(2016) 731 final.

przypadku których ryzyko uprowadzenia jest szczególnie duże. Zmiany te będą oznaczać, że funkcjonariusze straży granicznej i służby wymiaru sprawiedliwości zostaną powiadomieni w przypadku występowania dużego ryzyka rychłego uprowadzenia dziecka przez jednego z rodziców i będą w stanie dokładniej zbadać okoliczności podróży takiego dziecka, w razie potrzeby stosując wobec niego pieczę ochronną. Informacje uzupełniające, w tym decyzja właściwego organu sądowego, który zwrócił się o wprowadzenie wpisu, będą udzielane przez biura SIRENE. Przeprowadzony zostanie odpowiedni przegląd podręcznika SIRENE. Tego rodzaju wpis będzie wymagał odpowiedniej decyzji organów sądowych udzielających pieczy tylko jednemu rodzicowi. Kolejnym warunkiem będzie występowanie bezpośredniego ryzyka uprowadzenia. Status wpisów dotyczących zaginionego dziecka będzie w stosownych przypadkach automatycznie aktualizowany w momencie osiągnięcia przez dziecko pełnoletności.

Artykuł 34 dopuszcza uwzględnianie we wpisie danych dotyczących pojazdu, jeżeli istnieje wyraźna przesłanka, że dane te mają związek z poszukiwaną osobą.

Artykuł 37 wprowadza nową formę kontroli – „rozpytanie kontrolne”. Ma to na celu w szczególności wsparcie środków na rzecz zwalczania terroryzmu i poważnej przestępczości. W ramach tego rodzaju kontroli władze mogą zatrzymać i przesłuchać daną osobę. Tego rodzaju kontrola jest bardziej szczegółowa w porównaniu z kontrolą niejawną, nie obejmuje jednak przeszukania danej osoby ani nie oznacza jej aresztowania. W wyniku takiej kontroli można jednak uzyskać wystarczające informacje umożliwiające podjęcie decyzji w sprawie dalszego działania, które należy podjąć. Zmiany wprowadza się również w art. 36 w celu uwzględnienia przedmiotowego nowego rodzaju kontroli.

Zgodnie z niniejszym wnioskiem wpisy w SIS obejmują blankiety dokumentów urzędowych i wydane dokumenty tożsamości (art. 36) oraz pojazdy, w tym jednostki pływające i statki powietrzne (art. 32, 34), jeżeli tego rodzaju wpisy mają związek z wpisami dotyczącymi osób, wydanymi na podstawie tych artykułów. Artykuł 37 zostaje zmieniony, aby uwzględnić działanie podejmowane na podstawie tego rodzaju wpisów. Cel ten ma charakter czysto dochodzeniowy, ponieważ w ten sposób władze będą mogły zaradzić sytuacjom, w których kilka osób posługuje się autentycznymi, lecz podobnymi dokumentami, których nie są prawowitymi właścicielami.

Artykuł 38 zawiera rozszerzony wykaz przedmiotów, wobec których można dokonywać wpisów, do którego dodano: sfałszowane dokumenty, pojazdy niezależnie od systemu napędu (tj. niezależnie czy napędzane są silnikiem elektrycznym, spalinowym / silnikiem Diesla itp.), sfałszowane banknoty, sprzęt informatyczny oraz możliwe do identyfikacji komponenty pojazdów i urządzeń przemysłowych. W wykazie tym nie ma żadnych dłuższych wpisów dotyczących środków płatniczych, ponieważ ich skuteczność jest niewielka i rzadko dają one trafienia.

Celem wyjaśnienia procesu następującego po znalezieniu przedmiotu, którego dotyczy wpis, w art. 39 wprowadza się zmianę polegającą na stwierdzeniu, że oprócz skontaktowania się z organem, który wprowadził wpis, należy również zająć dane przedmioty zgodnie z prawem krajowym.

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 57).

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

Artykuł 12 zawiera również przepisy dotyczące automatycznego wyszukiwania opartego na skanowaniu tablic rejestracyjnych pojazdów silnikowych za pomocą systemów automatycznego rozpoznawania tablic rejestracyjnych, w których państwa członkowskie zobowiązuje się do prowadzenia rejestru tego rodzaju wyszukiwania zgodnie z prawem krajowym.

W art. 15 ust. 3 zachowuje się art. 15 ust. 3 decyzji Rady 2007/533/WSiSW, 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 należy zdecydować, czy dany przypadek jest wystarczająco stosowny, odpowiedni i ważny, tak aby wymóg ten miał również zastosowanie do decyzji w sprawie rozszerzenia okresu ważności wpisu. Jako nowy element w przedmiotowym artykule wymaga się, aby państwa członkowskie tworzyły wpis na podstawie (odpowiednio) art. 34, 36 i 38 we wszystkich okolicznościach w odniesieniu do osób, lub związanych z nimi przedmiotów, których działalność jest objęta zakresem stosowania art. 1, 2, 3 i 4 decyzji ramowej Rady 2002/475/WSiSW w sprawie zwalczania terroryzmu.

Kategorie danych i przetwarzanie danych

W niniejszym wniosku rozszerza się wykaz informacji (art. 20), które można przechowywać na temat osób, w odniesieniu do których wprowadzono wpis, 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;
- inne uwagi dotyczące danej osoby; powód wpisu;
- szczegółowe informacje na temat krajowego numeru rejestracyjnego danej osoby i miejsca rejestracji;
- kategoryzację rodzaju sprawy osoby zaginionej (wyłącznie wpisy, o których mowa w art. 32);
- szczegółowe informacje na temat dokumentu tożsamości lub dokumentu podróży danej osoby;
- kolorową kopię dokumentu tożsamości lub dokumentu podróży danej osoby;
- profile DNA (tylko wtedy, gdy odciski palców nadające się do identyfikacji są niedostępne).

W art. 59 wydłużono wykaz danych osobowych, jakie można wprowadzać do SIS i przetwarzać w tym systemie w celu rozwiązania problemów związanych z przywłaszczeniem tożsamości. Dane te można wprowadzić tylko za zgodą osoby, której tożsamość była przedmiotem 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 szczegółowe dane z dokumentów tożsamości osób, których dane dotyczą, oraz umożliwienie kategoryzacji zaginionych dzieci zgodnie z ich zniknięciem, np. małoletni bez opieki, uprowadzenie przez jednego z rodziców, ucieczka itd. W przypadku użytkowników końcowych konieczne jest niezwłoczne podjęcie wymaganych działań w celu ochrony tych dzieci. Rozszerzone informacje pozwalają na lepszą identyfikację danej osoby oraz na podjęcie bardziej świadomej decyzji przez użytkowników końcowych. W celu ochrony użytkowników końcowych prowadzących kontrolę 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 terroryzmu³⁴.

We wniosku wyraźnie stwierdzono, że państwa członkowskie nie mogą kopiować danych wprowadzonych przez inne państwo członkowskie do innych krajowych plików danych (art. 53).

Przechowywanie

Maksymalny okres przechowywania wpisów dotyczących danych osób zostanie wydłużony do pięciu lat, z wyjątkiem wpisów wykorzystywanych do prowadzenia kontroli niejawnych, szczególnych lub rozpytań kontrolnych, w przypadku których okres przechowywania trwa jeden rok. Państwa członkowskie zawsze mogą ustanowić krótsze okresy wygaśnięcia. Termin wygaśnięcia jest maksymalnie wydłużany zgodnie z praktykami krajowymi z zakresu wydłużania terminu wygaśnięcia, jeżeli cel wpisu nie został jeszcze osiągnięty, ponieważ dana osoba jest nadal poszukiwana. Ponadto konieczne było dostosowanie SIS do okresu przechowywania przewidzianego w innych instrumentach, takich jak dyrektywa powrotowa i Eurodac. W celu zachowania przejrzystości i jasności konieczne jest zapewnienie takiego samego okresu przechowywania wpisów dotyczących danych osób, z wyjątkiem wpisów utworzonych na potrzeby kontroli niejawnych, szczególnych lub rozpytań kontrolnych. Wydłużenie okresu przechowywania nie zagraża interesom osób, których dane dotyczą, ponieważ wpis nie może być przechowywany dłużej niż jest to konieczne dla osiągnięcia jego celu. Przepisy dotyczące usuwania wpisów wyraźnie określono w art. 52. W art. 51 przedstawiono ramy czasowe przeglądu wpisów oraz określono w szczególności skrócony okres przechowywania wpisów dotyczących przedmiotów. W przypadku braku jakiegokolwiek operacyjnej potrzeby utrzymania dłuższego okresu w odniesieniu do przedmiotów okres ten skrócono do pięciu lat w celu dostosowania go do okresu przechowywania wpisów dotyczących osób. Termin wygaśnięcia dokumentów i blankietów dokumentów nadal wynosi jednak 10 lat, ponieważ okres ważności dokumentów wynosi 10 lat.

Usuwanie

W art. 52 określono okoliczności, w których należy usunąć wpisy w celu zapewnienia większej harmonizacji praktyk krajowych w tej dziedzinie. W art. 51 określono szczególne przepisy umożliwiające personelowi biur SIRENE aktywne usuwanie niepotrzebnych wpisów 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

³⁴ 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).

Szczegółowe przepisy dotyczące praw osób, których dane dotyczą, pozostają niezmienione, ponieważ obowiązujące przepisy zapewniają już wysoki poziom ochrony i są zgodne z rozporządzeniem (UE) 2016/679³⁵ i dyrektywą 2016/680³⁶. Oprócz tego w art. 63 określono 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.

Udostępnianie Interpolowi danych na temat utraconych, skradzionych, unieważnionych i przywłaszczonych dokumentów

Artykuł 63 w pełni podtrzymuje art. 55 decyzji Rady 2007/533/WSiSW, jako że lepsza interoperacyjność między sekcją ds. dokumentów SIS a bazą danych Interpolu na temat skradzionych i utraconych dokumentów będzie przedmiotem komunikatu grupy ekspertów wysokiego szczebla i drugiego zestawu wniosków dotyczących SIS w czerwcu 2017 r.

Dane statystyczne

Aby śledzić sposób działania środków zaradczych w praktyce, w art. 66 określono przepis dotyczący standardowego systemu statystycznego zapewniającego 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. 71 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 71 ust. 5 wymaga, by eu-LISA przekazywała państwom członkowskim, Komisji, Europolowi, Eurojustowi 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.

³⁵ 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).

³⁶ 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).

W art. 71 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, Eurojustu i Europejskiej Agencji Straży Granicznej i Przybrzeżnej uzyskać dostęp do danych wymienionych w art. 71 ust. 3 w celu sporządzenia wymaganych statystyk.

Wniosek

ROZPORZĄDZENIE 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, zmieniające rozporządzenie (UE) nr 515/2014 i uchylające rozporządzenie (WE) nr 1986/2006, decyzję Rady 2007/533/WSiSW i decyzję Komisji 2010/261/UE

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 82 ust. 1 akapit drugi lit. d), art. 85 ust. 1, art. 87 ust. 2 lit. a) i art. 88 ust. 2 lit. a),

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 oraz innych organów ścigania i organów sądowniczych w sprawach karnych.
- (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 granicach³⁷ („konwencja z Schengen”). Opracowanie systemu SIS drugiej generacji (SIS II) powierzono Komisji na mocy rozporządzenia Rady (WE) nr 2424/2001³⁸ i decyzji Rady 2001/886/WSiSW³⁹; został on utworzony na mocy rozporządzenia (WE)

³⁷ 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).

³⁸ Dz.U. L 328 z 13.12.2001, s. 4.

³⁹ 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).

nr 1987/2006⁴⁰ i decyzji Rady 2007/533/WSiSW⁴¹. SIS II zastąpił SIS, który powstał na mocy konwencji z Schengen.

- (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.⁴². 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 rozdziałów 4 i 5 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 odpraw granicznych⁴³ stanowi niezbędną podstawę prawną dla systemu SIS w kwestiach objętych zakresem stosowania rozdziału 2 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

⁴⁰ 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).

⁴¹ 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).

⁴² 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. ...).

⁴³ Rozporządzenie (UE) 2018/...

poprzez określenie wymogów dotyczących dostępnych zasobów, szkoleń 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 Sprawiedliwości⁴⁴ („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 przestępstwami, 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. Dlatego też w celu ułatwienia identyfikacji osób i wykrycia wielorakich tożsamości kategorie danych dotyczących osób powinny 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.
- (16) Państwa członkowskie powinny dokonać niezbędnych ustaleń technicznych, tak aby za każdym razem użytkownicy końcowi byli uprawnieni do przeprowadzenia

⁴⁴ 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).

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) 2016/680⁴⁵. 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 odcisków palców i wizerunków twarzy. Wyszukiwanie na podstawie danych daktyloskopijnych powinno być obowiązkowe, jeżeli istnieją jakiegokolwiek 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) Usługa automatycznej identyfikacji daktyloskopijnej wprowadzona w ramach SIS stanowi uzupełnienie istniejącego mechanizmu Prüm dotyczącego wzajemnego transgranicznego dostępu online do wyznaczonych krajowych baz danych na temat DNA i systemów automatycznej identyfikacji daktyloskopijnej⁴⁶. Mechanizm Prüm umożliwia zapewnienie wzajemnych połączeń w ramach krajowych systemów identyfikacji daktyloskopijnej, przez co państwo członkowskie może wystąpić z wnioskiem o ustalenie, czy sprawca przestępstwa, którego odciski palców zostały znalezione, jest znany w innym państwie członkowskim. Mechanizm Prüm sprawdza, czy właściciel odcisków palców jest znany w danym czasie, dlatego jeżeli sprawca zostanie wykryty później w dowolnym innym państwie członkowskim, niekoniecznie zostanie zatrzymany. Dzięki wyszukiwaniu odcisków palców w SIS możliwe jest aktywne poszukiwanie sprawcy. W związku z powyższym powinno być możliwe przesłanie odcisków palców nieznanego sprawcy do SIS, pod warunkiem że istnieje duże prawdopodobieństwo, iż właściciela odcisków palców będzie można zidentyfikować jako sprawcę poważnego przestępstwa lub aktu terrorystycznego. W szczególności dotyczy to sytuacji, w której linie papilarne znajduje się na broni lub innym przedmiocie użytym do popełnienia przestępstwa. Nie należy przyjmować, że sama obecność linii papilarnych na miejscu przestępstwa wskazuje na wysokie prawdopodobieństwo, iż należą one do sprawcy. Kolejnym warunkiem utworzenia takiego wpisu powinien być fakt, że tożsamości sprawcy nie można ustalić za pomocą innych krajowych, europejskich lub międzynarodowych baz danych. Jeżeli wyszukiwane odciski palców pokryją się z odciskami dostępnymi w bazie danych, państwo członkowskie powinno przeprowadzić dalsze kontrole dotyczące odcisków

⁴⁵ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

⁴⁶ Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.U. L 210 z 6.8.2008, s. 1), oraz decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. w sprawie wdrożenia decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.U. L 210 z 6.8.2008, s. 12).

palców znajdujących się w jego bazie, ewentualnie z udziałem ekspertów daktyloskopijnych w celu ustalenia właściciela odcisków przechowywanych w SIS, oraz powinno ustalić tożsamość danej osoby. Procedury powinny być przedmiotem prawa krajowego. Identyfikacja „nieznanej osoby poszukiwanej” w SIS może znacznie wpłynąć na śledztwo i doprowadzić do aresztowania, o ile wszystkie warunki aresztowania zostały spełnione.

- (19) Należy umożliwić porównanie linii papilarnych znalezionych na miejscu przestępstwa z odciskami 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/WSiSW⁴⁷, zaś za „przestępstwa terrorystyczne” uznaje się przestępstwa w rozumieniu prawa krajowego, o których mowa w decyzji ramowej Rady 2002/475/WSiSW⁴⁸.
- (20) Powinna istnieć możliwość dodania profilu DNA w przypadkach, gdy dane daktyloskopijne są niedostępne, przy czym tylko upoważnieni użytkownicy powinni mieć dostęp do takich profili. Profile DNA powinny ułatwić identyfikację zaginionych osób potrzebujących ochrony, a w szczególności zaginionych dzieci, m.in. poprzez umożliwienie korzystania z profili DNA rodziców lub rodzeństwa w celu umożliwienia identyfikacji. Dane DNA nie powinny zawierać odniesienia do pochodzenia rasowego.
- (21) SIS powinien zawierać wpisy dotyczące osób poszukiwanych w celu aresztowania ich i wydania oraz osób poszukiwanych w celu aresztowania ich i ekstradycji. Celowe jest, aby oprócz wpisów zapewnić wymianę informacji uzupełniających, które są niezbędne w procedurach wydawania osób i ich ekstradycji. W SIS powinny być w szczególności przetwarzane dane, o których mowa w art. 8 decyzji ramowej Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi⁴⁹. Ze względów operacyjnych państwo członkowskie dokonujące wpisu powinno tymczasowo ograniczyć dostęp do istniejącego wpisu mającego doprowadzić do aresztowania na mocy upoważnienia organów sądowych, gdy osoba podlegająca europejskiemu nakazowi aresztowania jest intensywnie i aktywnie poszukiwana, a użytkownicy końcowi nieuczestniczący w konkretnej operacji poszukiwawczej mogą zagrozić pomyślnemu wynikowi tej operacji. Tymczasowe ograniczenie dostępu do takich wpisów nie powinno przekroczyć 48 godzin.
- (22) Powinna istnieć możliwość umieszczenia w SIS tłumaczenia danych dodatkowych, które są wprowadzane do celów związanych z wydawaniem osób na podstawie europejskiego nakazu aresztowania i ich ekstradycją.
- (23) SIS powinien zawierać wpisy dotyczące osób zaginionych, by zapewnić im ochronę lub wyeliminować zagrożenia dla bezpieczeństwa publicznego. Dodawanie wpisów do SIS dotyczących dzieci zagrożonych uprowadzeniem (tj. w celu uniknięcia przyszłych

⁴⁷ 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).

⁴⁸ 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).

⁴⁹ 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).

szkód, które jeszcze nie miały miejsca, jak w przypadku dzieci zagrożonych uprowadzeniem przez jednego z rodziców) powinno być ograniczone, dlatego wskazane jest zapewnienie rygorystycznych i odpowiednich zabezpieczeń. W przypadku dzieci wpisy te i odpowiednie procedury powinny mieć na celu najlepsze zabezpieczenie interesu dziecka, uwzględniając art. 24 Karty praw podstawowych Unii Europejskiej oraz Konwencję ONZ o prawach dziecka z dnia 20 listopada 1989 r.

- (24) Nowe działanie należy uwzględnić w przypadkach podejrzenia popełnienia przestępstwa terrorystycznego i poważnego przestępstwa, umożliwiając zatrzymanie i przesłuchanie osoby podejrzanej o popełnienie poważnego przestępstwa lub w przypadku której istnieje powód, by przypuszczać, że popełni poważne przestępstwo, w celu przekazania najbardziej szczegółowych informacji państwu członkowskiemu dokonującemu wpisu. Takie nowe działanie nie powinno być równoznaczne z poszukiwaniem danej osoby lub jej aresztowaniem. Należy dostarczyć jednak informacje wystarczające do podjęcia decyzji o dalszych działaniach. Za „poważne przestępstwo” należy uznać przestępstwa wymienione w decyzji ramowej Rady 2002/584/WSiSW.
- (25) SIS powinien zawierać nowe kategorie przedmiotów o znacznej wartości, takich jak sprzęt elektroniczny i techniczny, które można zidentyfikować i wyszukiwać po unikalnym numerze.
- (26) Państwo członkowskie powinno mieć możliwość umieszczenia przy wpisie wskazówki, zwanej zastrzeżeniem, że działanie, które należy podjąć w myśl wpisu, nie będzie podjęte na terytorium tego państwa. W odniesieniu do wpisów mających prowadzić do aresztowania i wydania osób – żaden z przepisów niniejszej decyzji nie powinien być interpretowany jako odstępstwo od przepisów decyzji ramowej 2002/584/WSiSW lub przeszkoda w ich stosowaniu. Decyzja o umieszczeniu przy wpisie zastrzeżenia powinna być uzasadniona jedynie tymi powodami odmowy, które zawarte są we wspomnianej decyzji ramowej.
- (27) W przypadku umieszczenia zastrzeżenia, gdy ustalono miejsce pobytu osoby poszukiwanej w celu aresztowania jej i wydania, o miejscu tym powinien być zawsze powiadamiany organ sądowy wydający nakaz, który może podjąć decyzję o przekazaniu europejskiego nakazu aresztowania właściwemu organowi sądowemu zgodnie z przepisami decyzji ramowej 2002/584/WSiSW.
- (28) 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.
- (29) Wpisów nie należy przechowywać w SIS dłużej, niż jest to konieczne do osiągnięcia celów, w jakich zostały dodane. Aby zmniejszyć obciążenia administracyjne różnych organów zaangażowanych w przetwarzanie danych na temat poszczególnych osób do różnych celów, należy dostosować okres przechowywania wpisów dotyczących danych osób do okresów przechowywania przewidzianych do celów powrotu i nielegalnego pobytu. Ponadto państwa członkowskie regularnie przedłużają termin ważności wpisów dotyczących osób, jeżeli nie można podjąć wymaganego działania w pierwotnym terminie. 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, z wyjątkiem wpisów wprowadzonych w celu przeprowadzenia kontroli niejawnych, szczególnych lub rozpytań kontrolnych. Takie wpisy należy usunąć po upływie roku. Wpisy

dotyczące przedmiotów dokonane z myślą o kontrolach niejawnych, szczególnych lub rozpytaniach kontrolnych powinny być automatycznie usuwane z SIS po upływie roku, ponieważ zawsze są związane z osobami. Wpisy dotyczące przedmiotów przeznaczonych do zajęcia lub wykorzystania jako dowód w postępowaniu karnym powinny być automatycznie usuwane z SIS po upływie pięciu lat, ponieważ po takim okresie prawdopodobieństwo znalezienia tych przedmiotów jest bardzo małe, a ich wartość ekonomiczna znacznie zmniejszona. Wpisy dotyczące dokumentów tożsamości i blankietów dokumentów tożsamości należy przechowywać przez 10 lat, ponieważ okres ważności takich dokumentów wynosi 10 lat od czasu wydania. 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.

- (30) 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. Przestępstwa, o których mowa w art. 1, 2, 3 i 4 decyzji ramowej Rady 2002/475/WSiSW w sprawie zwalczania terroryzmu⁵⁰, stanowią bardzo poważne zagrożenie dla bezpieczeństwa publicznego i integralności życia poszczególnych osób oraz dla społeczeństwa, przy czym niezwykle trudno jest zapobiegać tym przestępstwom, wykrywać je i ścigać na obszarze bez wewnętrznych kontroli granicznych, po którym potencjalni przestępcy mogą się swobodnie przemieszczać. Jeżeli dana osoba lub przedmiot są poszukiwane w związku z tymi przestępstwami, zawsze konieczne jest utworzenie odpowiedniego wpisu w SIS dotyczącego osób poszukiwanych w ramach postępowania sądowego w sprawie karnej, osób lub przedmiotów podlegających kontroli niejawnej, szczególnej i rozpytaniu kontrolnemu oraz dotyczącego przedmiotów przeznaczonych do zajęcia, ponieważ żadne inne środki nie byłyby skuteczne w odniesieniu do tego celu.
- (31) Konieczne jest zapewnienie jasności co do usuwania wpisów. Wpisy należy przechowywać wyłącznie przez okres konieczny dla osiągnięcia celu, w którym zostały wprowadzone. Biorąc pod uwagę rozbieżne praktyki państw członkowskich w definiowaniu momentu, w którym wpis spełnia swój cel, należy określić szczegółowe kryteria służące do ustalenia, kiedy poszczególne kategorie wpisów powinny być usuwane z SIS.
- (32) 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 uczestniczące w przetwarzaniu danych powinny być objęte wymogami bezpieczeństwa określonymi w niniejszym rozporządzeniu i podlegać jednolitej procedurze zgłaszania incydentów.
- (33) Dane przetwarzane w SIS na użytek niniejszego rozporządzenia nie powinny być przekazywane ani udostępniane państwom trzecim ani organizacjom międzynarodowym. Celowe jest jednak, by zacieśnić współpracę między Unią Europejską a Interpołem przez propagowanie efektywnej wymiany danych

⁵⁰

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).

paszportowych. W przypadku przekazywania danych osobowych z SIS Interpolowi powinny być one objęte ochroną o odpowiednim poziomie, zagwarantowaną porozumieniem przewidującym ściśle zabezpieczenia i warunki.

- (34) Wskazane jest przyznanie dostępu do SIS organom odpowiedzialnym za rejestrowanie pojazdów, jednostek pływających i statków powietrznych, aby umożliwić im sprawdzenie, czy dany środek transportu poszukiwany był już w państwach członkowskich na potrzeby zajęcia lub kontroli. Bezpośredni dostęp należy zapewnić organom pełniącym rolę służb państwowych. Dostęp ten należy ograniczyć do wpisów dotyczących odnośnych środków transportu oraz ich dokumentów rejestracyjnych lub tablic rejestracyjnych. W związku z powyższym przepisy rozporządzenia (WE) nr 1986/2006 Parlamentu Europejskiego i Rady⁵¹ należy włączyć do niniejszego rozporządzenia, a wspomniane rozporządzenie należy uchylić.
- (35) W przypadku przetwarzania danych przez właściwe organy krajowe do celów zapobiegania poważnym przestępstwom lub przestępstwom terrorystycznym, prowadzenia postępowań przygotowawczych w ich sprawie oraz ich wykrywania lub ścigania czynów zabronionych i wykonywania kar, w tym zapobiegania zagrożeniom dla bezpieczeństwa publicznego, zastosowanie powinny mieć przepisy krajowe transponujące dyrektywę (UE) 2016/680. Przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679⁵² i dyrektywy (UE) 2016/680 należy, w stosownych przypadkach, doprecyzować w niniejszym rozporządzeniu.
- (36) Rozporządzenie (UE) 2016/679 powinno mieć zastosowanie do przetwarzania danych osobowych przez organy krajowe na mocy niniejszego rozporządzenia, gdy dyrektywa (UE) 2016/680 nie ma zastosowania. Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady⁵³ powinno mieć zastosowanie do przetwarzania danych osobowych przez instytucje i organy unijne podczas wykonywania przez nie swoich obowiązków na mocy niniejszego rozporządzenia.
- (37) 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 (rozporządzenie w sprawie Europolu)⁵⁴.

⁵¹ Rozporządzenie (WE) nr 1986/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie dostępu służb odpowiedzialnych w państwach członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 381 z 28.12.2006, s. 1).

⁵² 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).

⁵³ 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).

⁵⁴ 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).

- (38) Przepisy decyzji 2002/187/WSiSW z dnia 28 lutego 2002 r.⁵⁵ ustanawiającej Eurojust w celu zintensyfikowania walki z poważną przestępczością, które dotyczą ochrony danych, mają zastosowanie do przetwarzania danych SIS przez Eurojust, w tym do uprawnień wspólnego organu nadzorczego utworzonego na podstawie wspomnianej decyzji w zakresie monitorowania działań oraz jego odpowiedzialności w razie niezgodnego z prawem przetwarzania danych osobowych przez Eurojust. Jeżeli w wyniku wyszukiwania w SIS Eurojust 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.
- (39) 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.
- (40) 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.
- (41) 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.
- (42) 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 prowadzić 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.
- (43) 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. Rozszerzenie praw dostępu Europolu do wpisów SIS dotyczących osób zaginionych powinno dodatkowo poprawić zdolności Europolu w zakresie dostarczania krajowym organom ścigania kompleksowych produktów operacyjnych i analitycznych dotyczących handlu ludźmi i wykorzystywania seksualnego dzieci, m.in. za pośrednictwem internetu. Przyczyni się to do efektywniejszego zapobiegania tym przestępstwom, ochrony potencjalnych ofiar i ścigania sprawców. Europejskie Centrum ds. Walki z Cyberprzestępczością działające przy Europolu także skorzysta z

⁵⁵

Decyzja Rady 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz.U. L 63 z 6.3.2002, s. 1).

nowego dostępu Europolu do wpisów SIS dotyczących osób zaginionych, m.in. w przypadku podróżujących przestępców seksualnych i niegodziwego traktowania dzieci w internecie w celach seksualnych, gdy sprawcy często twierdzą, że mają dostęp do dzieci lub mogą uzyskać dostęp do dzieci zarejestrowanych jako zaginione. Ponadto, ponieważ Europejskie Centrum Zwalczenia Przemytu Migrantów działające przy Europolu odgrywa ważną rolę strategiczną w zwalczaniu ułatwiania nielegalnej migracji, należy 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 uzyskania wizy i warunków pobytu.

- (44) 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 równoległe z wprowadzaniem wpisów do SIS, a także informacje o trafieniach i powiązane informacje. Powinno to umożliwić Europejskiemu Centrum ds. Zwalczenia 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.
- (45) 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.
- (46) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624⁵⁶ 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 zespołu wspierającego zarządzanie migracjami jest zapewnienie wzmocnienia

⁵⁶ 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).

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 zespołowi wspierającemu 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.

- (47) Zgodnie z wnioskiem Komisji dotyczącym rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)⁵⁷ 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 zezwolenie na podróż. W tym celu jednostka centralna ETIAS w ramach Europejskiej Agencji Straży Granicznej i Przybrzeżnej powinna mieć również dostęp do SIS w zakresie niezbędnym do wykonania swojego mandatu, czyli do wszystkich kategorii osób i wpisów dotyczących blankietów dokumentów tożsamości i wydanych dokumentów tożsamości.
- (48) 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 zgodności i kolejności wpisów, dodawania zastrzeżeń, odsyłaczy do innych wpisów, określania nowych kategorii przedmiotów w obrębie kategorii sprzętu technicznego i elektronicznego, 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.
- (49) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011⁵⁸. Procedury przyjmowania środków wykonawczych na mocy niniejszego rozporządzenia i rozporządzenia (UE) 2018/xxx (odprawy graniczne) powinny być takie same.
- (50) 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.

⁵⁷ COM(2016) 731 final.

⁵⁸ 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).

- (51) 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.
- (52) 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 objęcie szczególną ochroną dzieci, które mogą stać się ofiarą handlu ludźmi lub zostać uprowadzone przez jednego z rodziców, przy pełnym poszanowaniu ochrony danych osobowych.
- (53) 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.
- (54) Zjednoczone Królestwo uczestniczy w niniejszym rozporządzeniu zgodnie z art. 5 Protokołu w sprawie dorobku Schengen włączonego w ramy Unii Europejskiej, załączonego do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, oraz z art. 8 ust. 2 decyzji Rady 2000/365/WE z dnia 29 maja 2000 r. dotyczącej wniosku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o zastosowaniu wobec niego niektórych przepisów dorobku Schengen⁵⁹.
- (55) Irlandia uczestniczy w niniejszym rozporządzeniu zgodnie z art. 5 Protokołu w sprawie dorobku Schengen włączonego w ramy Unii Europejskiej, załączonego do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, oraz z art. 6 ust. 2 decyzji Rady 2002/192/WE z dnia 28 lutego 2002 r. dotyczącej wniosku Irlandii o zastosowanie wobec niej niektórych przepisów dorobku Schengen⁶⁰.
- (56) 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 Schengen⁶¹ – które należą do dziedziny, o której mowa w art. 1 lit. G decyzji Rady 1999/437/WE⁶² w sprawie niektórych warunków stosowania tego układu.
- (57) 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

⁵⁹ Dz.U. L 131 z 1.6.2000, s. 43.

⁶⁰ Dz.U. L 64 z 7.3.2002, s. 20.

⁶¹ Dz.U. L 176 z 10.7.1999, s. 36.

⁶² Dz.U. L 176 z 10.7.1999, s. 31.

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/WE⁶³ oraz 2004/860/WE⁶⁴.

- (58) 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 Schengen⁶⁵, które wchodzi w zakres obszaru, o którym mowa w art. 1 lit. G decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2011/349/UE⁶⁶ i art. 3 decyzji Rady 2011/350/UE⁶⁷.
- (59) 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 Schengen⁶⁸.
- (60) 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.
- (61) Niniejsze rozporządzenie powinno mieć zastosowanie wobec Irlandii od dnia określonego według procedur, o których mowa w odnośnych aktach dotyczących stosowania prawnego dorobku Schengen wobec tego państwa.
- (62) 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 515/2014⁶⁹. W związku z powyższym w niniejszym rozporządzeniu należy ponownie przydzielić kwotę

⁶³ 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).

⁶⁴ 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).

⁶⁵ Dz.U. L 160 z 18.6.2011, s. 21.

⁶⁶ 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).

⁶⁷ 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).

⁶⁸ Dz.U. L 166 z 1.7.2010, s. 17.

⁶⁹ 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).

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.

- (63) Należy zatem uchylić decyzję Rady 2007/533/WSiSW i decyzję Komisji 2010/261/UE⁷⁰.
- (64) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu [...] r.,

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 rozdziały 4 i 5 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 wpisów w SIS dotyczących osób i przedmiotów oraz wymiany informacji uzupełniających i danych dodatkowych w celach związanych ze współpracą policyjną i współpracą wymiarów sprawiedliwości w sprawach karnych.
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 i w art. 40, wprowadzonych do SIS, umożliwiających

⁷⁰ 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).

właściwym organom zidentyfikowanie osoby lub przedmiotu 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) „dane osobowe” oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoba, której dotyczą dane”);
- e) „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;
- f) „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;
- g) „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) wymagane jest podjęcie dalszych działań;

- h) „zastrzeżenie” oznacza zawieszenie ważności wpisu na poziomie krajowym, które można umieścić przy wpisach mających doprowadzić do aresztowania, wpisach dotyczących osób zaginionych oraz wpisach wykorzystywanych do prowadzenia kontroli niejawnych, szczególnych i rozpytań kontrolnych, jeżeli państwo członkowskie uważa, że wykonanie czynności wymaganych we wpisie jest niezgodne z jego prawem krajowym, jego zobowiązaniami międzynarodowymi lub podstawowymi interesami krajowymi. Jeżeli przy danym wpisie umieszczono zastrzeżenie, działania wymagane na podstawie wspomnianego wpisu nie są podejmowane na obszarze danego państwa członkowskiego;
- i) „państwo członkowskie dokonujące wpisu” oznacza państwo członkowskie, które dokonało wpisu w SIS;
- j) „państwo członkowskie wykonujące wpis” oznacza państwo członkowskie, które podejmuje lub podjęło 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) „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;
- m) „poważne przestępstwo” oznacza przestępstwa wymienione w art. 2 ust. 1 i 2 decyzji ramowej 2002/584/WSiSW z dnia 13 czerwca 2002 r.⁷¹;
- n) „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.⁷².

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

⁷¹ 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).

⁷² 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 zaszyfowaną 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 dotyczące przedmiotów i danych wymienionych w art. 20 ust. 3 lit. a)–v) niniejszego rozporządzenia w odniesieniu do wpisów dotyczących osób. 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 1077/2011⁷³ („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.
- 3. Koszty budowy, eksploatacji, utrzymania i dalszego rozwoju każdego N.SIS ponosi dane państwo członkowskie.

⁷³ 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).

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. 53 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. 61, 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. 72 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 przyjmuje się w drodze środków wykonawczych zgodnie z procedurą sprawdzającą określoną w art. 72 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 posiadaniem 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. 66, 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 przetwarzania 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. 43.

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, dane wykorzystane do wyszukiwania, odniesienie do danych przekazanych 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. 40, 41 i 42, 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, 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.
7. Jeżeli państwa członkowskie przeprowadzają automatyczne wyszukiwania oparte na skanowaniu tablic rejestracyjnych pojazdów silnikowych, korzystając z systemów automatycznego rozpoznawania tablic rejestracyjnych, państwa członkowskie prowadzą rejestr wyszukiwania zgodnie z prawem krajowym. Zawartość tego rejestru określa się w drodze środków wykonawczych zgodnie z procedurą sprawdzającą określoną w art. 72 ust. 2. Jeżeli uzyskano dopasowanie pozytywne w odniesieniu do danych przechowywanych w SIS lub w odniesieniu do kopii krajowej lub technicznej danych SIS, w SIS przeprowadza się pełne wyszukiwanie w celu sprawdzenia, czy faktycznie uzyskano dopasowanie pozytywne. Przepisy ust. 1–6 niniejszego artykułu mają zastosowanie do wspomnianego pełnego wyszukiwania.

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 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 w drodze środków wykonawczych zgodnie z procedurą sprawdzającą określoną w art. 72 ust. 2.

6. Zarządzanie operacyjne centralnym SIS obejmuje wszystkie zadania niezbędne do tego, by centralny SIS działał 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 posiadaniem 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. 64, na jego wniosek (profile personelu);
 - h) zapewnić możliwość weryfikacji i stwierdzenia, jakim organom można przekazywać dane osobowe za pośrednictwem sprzętu do przekazywania danych (kontrola przekazywania danych);
 - i) zapewnić następnie możliwość weryfikacji i stwierdzenia, 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. 40, 41 i 42, 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

KATEGORIE DANYCH I UMIESZCZANIE ZASTRZEŻEŃ

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. 26, 32, 34, 36 i 38.
2. Dane te dzielą się na następujące kategorie:
 - a) informacje na temat osób, w odniesieniu do których został dokonany wpis;
 - b) informacje na temat przedmiotów, o których mowa w art. 32, 36 i 38.
3. 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. 53;
 - p) rodzaj przestępstwa, w odniesieniu do którego utworzono wpis;
 - q) numer rejestracyjny danej osoby w rejestrze krajowym;
 - r) kategorię rodzaju sprawy osoby zaginionej (wyłącznie w odniesieniu do wpisów, o których mowa w art. 32);
 - 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) odpowiednie profile DNA z zastrzeżeniem art. 22 ust. 1 lit. b) niniejszego rozporządzenia;
 - y) dane daktyloskopijne;
 - z) kolorową kopię dokumentu identyfikacyjnego.
4. Techniczne zasady wpisywania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 2 i 3, określa się i opracowuje w drodze środków wykonawczych zgodnie z procedurą sprawdzającą, o której mowa w art. 72 ust. 2.
5. Techniczne zasady wyszukiwania danych, o których mowa w ust. 3, określa się i opracowuje zgodnie z procedurą sprawdzającą, o której mowa w art. 72 ust. 2. Wspomniane techniczne zasady są podobne do zasad wyszukiwania w CS-SIS, w kopiach krajowych i technicznych, o których mowa w art. 53 ust. 2, a ich podstawę stanowią wspólne normy określone i opracowane w drodze środków wykonawczych zgodnie z procedurą sprawdzającą, o której mowa w art. 72 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. Jeżeli państwo członkowskie poszukuje osoby lub przedmiotu w związku z przestępstwem, które jest objęte zakresem stosowania art. 1–4 decyzji ramowej Rady 2002/475/WSiSW w sprawie zwalczania terroryzmu, państwo członkowskie we wszystkich sytuacjach tworzy odpowiedni wpis na mocy odpowiednio art. 34, 36 albo 38.

Artykuł 22

Zasady szczególowe dotyczące wprowadzania fotografii, obrazów twarzy, danych daktyloskopijnych i profili DNA

1. Wprowadzenie do SIS danych, o których mowa w art. 20 ust. 3 lit. w), x) i y), podlega następującym przepisom:
 - a) fotografie, obrazy twarzy, dane daktyloskopijne i profile DNA wprowadzane są dopiero po przeprowadzeniu kontroli jakości stwierdzającej, czy spełniają minimalny standard jakości danych;
 - b) profil DNA można dodać wyłącznie do wpisów, o których mowa w art. 32 ust. 2 lit. a) i c), oraz wyłącznie w przypadku, gdy fotografie, obrazy twarzy lub dane daktyloskopijne umożliwiające identyfikację nie są dostępne. Profile DNA osób będących bezpośrednimi wstępnymi, zstępnymi lub rodzeństwem osoby, której dotyczy wpis, mogą zostać dodane do wpisu pod warunkiem, że osoby te wyrażą wyraźną zgodę. W profilu DNA nie uwzględnia się pochodzenia rasowego osoby.
2. Należy ustanowić normy jakości w odniesieniu do przechowywania danych, o których mowa w ust. 1 lit. a) niniejszego artykułu oraz w art. 40. Specyfikację tych norm określa się w drodze środków wykonawczych i aktualizuje zgodnie z procedurą sprawdzającą określoną w art. 72 ust. 2.

Artykuł 23

Wymóg warunkujący dokonanie wpisu

1. Wpisu na temat osoby nie wolno dokonywać, jeżeli brak jest danych, o których mowa w art. 20 ust. 3 lit. a), g), k), m) i n) oraz w stosownych przypadkach w art. 20 ust. 3 lit. p), z wyjątkiem sytuacji, o których mowa w art. 40.
2. Wprowadzane są również wszystkie pozostałe dane wymienione w art. 20 ust. 3, o ile są dostępne.

Artykuł 24

Przepisy ogólne o umieszczaniu zastrzeżeń

1. Jeżeli państwo członkowskie uważa, że wykonanie czynności wymaganych we wpisie dokonanym zgodnie z art. 26, 32 i 36 jest niezgodne z jego prawem krajowym, jego zobowiązaniami międzynarodowymi lub podstawowymi interesami narodowymi, państwo to może zażądać umieszczenia przy wpisie zastrzeżenia wskazującego, że działanie, które należy podjąć na podstawie wpisu, nie będzie podjęte na terytorium tego państwa. Zastrzeżenie jest dodawane przez biuro SIRENE państwa członkowskiego dokonującego wpisu.
2. W celu umożliwienia państwom członkowskim żądania umieszczenia zastrzeżenia przy wpisie dokonanym zgodnie z art. 26, wszystkie państwa członkowskie są – w

drodze wymiany informacji uzupełniających – automatycznie informowane o każdym nowym wpisie tej kategorii.

3. Jeżeli w szczególnie pilnych i poważnych przypadkach państwo członkowskie dokonujące wpisu zażąda wykonania danego działania, państwo członkowskie wykonujące wpis bada, czy może zezwolić na usunięcie zastrzeżenia umieszczonego przy wpisie na jego wniosek. Jeżeli państwo członkowskie wykonujące wpis jest w stanie to uczynić, podejmuje niezbędne kroki, by żądane działania zostały przeprowadzone niezwłocznie.

Artykuł 25

Zastrzeżenia przy wpisach mających prowadzić aresztowania osób w celu ich wydania

1. Jeżeli zastosowanie ma decyzja ramowa 2002/584/WSiSW, zastrzeżenie zapobiegające aresztowaniu jest umieszczane przy wpisie mającym doprowadzić do aresztowania i wydania osoby wyłącznie w przypadku, gdy odmowa organu sądowego właściwego według prawa krajowego w sprawach wykonania europejskiego nakazu aresztowania opiera się na podstawie odmowy wykonania oraz gdy zażądano umieszczenia zastrzeżenia.
2. O umieszczenie zastrzeżenia przy wpisie mającym doprowadzić do aresztowania osoby w celu jej wydania może wystąpić właściwy według prawa krajowego organ sądowy na podstawie ogólnej instrukcji lub w konkretnej sprawie, jeżeli jest oczywiste, że konieczna będzie odmowa wykonania europejskiego nakazu aresztowania.

ROZDZIAŁ VI

WPISY DOTYCZĄCE OSÓB POSZUKIWANYCH W CELU ARESztOWANIA ICH I WYDANIA LUB EKSTRADYCJI

Artykuł 26

Cele i warunki dokonywania wpisów

1. Dane osób poszukiwanych w celu aresztowania ich i wydania na podstawie europejskiego nakazu aresztowania lub osób poszukiwanych w celu aresztowania ich i ekstradycji są wprowadzane na wniosek właściwego organu sądowego państwa członkowskiego dokonującego wpisu.
2. Dane osób poszukiwanych w celu aresztowania ich i wydania są wprowadzane również na podstawie nakazów aresztowania wydawanych zgodnie z umowami, które Unia zawarła z państwami trzecimi na podstawie art. 37 Traktatu o Unii Europejskiej w celach związanych z wydawaniem osób na podstawie nakazu aresztowania i które przewidują przekazywanie takiego nakazu aresztowania za pośrednictwem SIS.
3. W przypadku odesłania w niniejszym rozporządzeniu do przepisów decyzji ramowej 2002/584/WSiSW uznaje się, że zastosowanie mają także odpowiednie postanowienia umów, które Unia Europejska zawarła z państwami trzecimi na podstawie art. 37 Traktatu o Unii Europejskiej w celach związanych z wydawaniem osób na podstawie nakazu aresztowania, które przewidują przekazywanie takiego nakazu aresztowania za pośrednictwem SIS.

4. W przypadku trwającej operacji wyszukiwania i po uzyskaniu pozwolenia właściwego organu sądowego państwa członkowskiego dokonującego wpisu państwo członkowskie dokonujące wpisu może tymczasowo zawiesić możliwość wyszukania istniejącego wpisu mającego doprowadzić do aresztowania, dokonanego zgodnie z art. 26 niniejszego rozporządzenia, w wyniku czego wyszukanie tego wpisu przez użytkownika końcowego stanie się niemożliwe, a dostęp do niego będą miały wyłącznie biura SIRENE. Z funkcji tej korzysta się przez okres nie dłuższy niż 48 godzin. Jeżeli jednak jest to konieczne z operacyjnego punktu widzenia, okres ten można wydłużyć o kolejne wielokrotności 48 godzin. Państwa członkowskie przechowują statystyki dotyczące liczby wpisów, w odniesieniu do których zastosowano tę funkcję.

Artykuł 27

Dane dodatkowe dotyczące osób poszukiwanych w celu aresztowania ich i wydania

1. Jeżeli osoba jest poszukiwana w celu aresztowania jej i wydania na podstawie europejskiego nakazu aresztowania, państwo członkowskie wydające nakaz wprowadza do SIS kopię oryginału europejskiego nakazu aresztowania.
2. Państwo członkowskie dokonujące wpisu może wprowadzić do systemu kopię tłumaczenia europejskiego nakazu aresztowania na co najmniej jeden z języków urzędowych instytucji Unii Europejskiej.

Artykuł 28

Informacje uzupełniające o osobach poszukiwanych w celu aresztowania ich i wydania

Państwo członkowskie, które wprowadziło do SIS wpis mający doprowadzić do aresztowania i wydania osoby, przekazuje informacje, o których mowa w art. 8 ust. 1 decyzji ramowej 2002/584/WSiSW, pozostałym państwom członkowskim w drodze wymiany informacji uzupełniających.

Artykuł 29

Informacje uzupełniające o osobach poszukiwanych w celu aresztowania ich i ekstradycji

1. Państwo członkowskie, które wprowadziło do SIS wpis mający doprowadzić do ekstradycji, przekazuje pozostałym państwom członkowskim w drodze wymiany informacji dodatkowych następujące dane:
 - a) organ, który wydał wniosek o aresztowanie;
 - b) informację, czy istnieje nakaz aresztowania lub dokument mający identyczny skutek prawny lub podlegający wykonaniu wyrok;
 - c) kategorię i kwalifikację prawną przestępstwa;
 - d) opis okoliczności, w których przestępstwo zostało popełnione, w tym czas, miejsce oraz formę udziału osoby, w odniesieniu do której wpis został wprowadzony, w popełnieniu przestępstwa;
 - e) w zakresie, w jakim jest to możliwe, konsekwencje popełnienia przestępstwa;
 - f) wszelkie inne informacje użyteczne lub niezbędne do tego, by wykonać czynności wymagane we wpisie.

2. Dane wymienione w ust. 1 nie są przekazywane, jeżeli dane, o których mowa w art. 27 lub 28, zostały już dostarczone i zostały uznane za wystarczające do tego, by dane państwo członkowskie wykonało czynności wymagane we wpisie.

Artykuł 30

Przekształcanie wpisów dotyczących osób poszukiwanych w celu aresztowania ich i wydania lub ekstradycji

Jeżeli aresztowanie nie może dojść do skutku, z uwagi na odmowę przez wezwane państwo członkowskie zgodnie z procedurami dotyczącymi wprowadzania zastrzeżeń określonymi w art. 24 lub 25 albo z uwagi na to, iż nie zakończyło się dochodzenie w związku z wpisem wymagającym aresztowania i ekstradycji osoby, wezwane państwo uznaje dany wpis za dotyczący podania miejsca pobytu danej osoby.

Artykuł 31

Wykonanie działania na podstawie wpisu dotyczącego osoby poszukiwanej w celu aresztowania jej i wydania lub ekstradycji

1. W przypadkach, w których ma zastosowanie decyzja ramowa 2002/584/WSiSW, wpis dokonany w SIS zgodnie z art. 26 wraz z danymi dodatkowymi, o których mowa w art. 27, stanowią europejski nakaz aresztowania wydany zgodnie z decyzją ramową 2002/584/WSiSW i mają taki sam skutek.
2. Jeżeli decyzja ramowa 2002/584/WSiSW nie ma zastosowania, wpis dokonany w SIS zgodnie z art. 26 i art. 29 ma taki sam skutek prawny, co wniosek o tymczasowe aresztowanie wydany na podstawie art. 16 Europejskiej konwencji o ekstradycji z dnia 13 grudnia 1957 r. lub art. 15 Traktatu o ekstradycji oraz pomocy prawnej w sprawach karnych z dnia 27 czerwca 1962 r.

ROZDZIAŁ VII

WPISY DOTYCZĄCE OSÓB ZAGINIONYCH

Artykuł 32

Cele i warunki dokonywania wpisów

1. Dane osób zaginionych lub innych osób, które powinny być objęte ochroną lub osób, których miejsce przebywania należy ustalić, są wprowadzane do SIS na wniosek właściwego organu państwa członkowskiego dokonującego wpisu.
2. Wprowadzane mogą być następujące kategorie osób zaginionych:
 - a) osoby zaginione, które muszą być objęte ochroną:
 - (i) dla ich własnej ochrony;
 - (ii) w celu zapobiegania zagrożeniom;
 - a) osoby zaginione, które nie muszą być objęte ochroną;
 - b) dzieci zagrożone uprowadzeniem zgodnie z ust. 4.
3. Ustęp 2 lit. a) ma zastosowanie w szczególności do dzieci, które muszą zostać umieszczone w odpowiedniej placówce w wyniku decyzji podjętej przez właściwy organ.

4. Wpisu dotyczącego dziecka, o którym mowa w ust. 2 lit. c), dokonuje się na wniosek właściwego organu sądowego państwa członkowskiego właściwego do spraw dotyczących odpowiedzialności rodzicielskiej zgodnie z rozporządzeniem Rady nr 2201/2003⁷⁴, jeżeli istnieje wyraźne i widoczne ryzyko, że dziecko może zostać niezgodnie z prawem i rychle wywiezione z państwa członkowskiego, w którym znajduje się siedziba danego organu sądowego. W państwach członkowskich będących stroną haskiej Konwencji z dnia 19 października 1996 r. o jurysdykcji, prawie właściwym, uznawaniu, wykonywaniu i współpracy w zakresie odpowiedzialności rodzicielskiej oraz środków ochrony dzieci oraz w przypadkach, gdy rozporządzenie nr 2201/2003 nie obowiązuje, zastosowanie mają przepisy konwencji haskiej.
5. Państwa członkowskie zapewniają, by dane wprowadzane do SIS wskazywały, do której z kategorii wymienionych w ust. 2 należy dana zaginiona osoba. Ponadto państwa członkowskie zapewniają również, by dane wprowadzane do SIS wskazywały, do której kategorii spraw dotyczących osób zaginionych lub osób wymagających szczególnego traktowania należy dana sprawa. Zasady kategoryzacji typów spraw i wprowadzania takich danych określa się i opracowuje w drodze środków wykonawczych zgodnie z procedurą sprawdzającą określoną w art. 72 ust. 2.
6. Cztery miesiące przed osiągnięciem pełnoletności przez dziecko, którego dotyczy wpis, CS-SIS automatycznie powiadamia państwo członkowskie dokonujące wpisu o konieczności aktualizacji podstaw wniosku oraz działania, które ma zostać podjęte, lub o konieczności usunięcia wpisu.
7. W przypadku gdy istnieje wyraźne wskazanie, że pojazdy, jednostki pływające lub statki powietrzne są powiązane z osobą, której dotyczy wpis wydany zgodnie z ust. 2, wydane mogą zostać wpisy dotyczące tych pojazdów, łodzi i statków powietrznych w celu zlokalizowania danej osoby. W takich przypadkach wpis dotyczący osoby zaginionej oraz wpis dotyczący przedmiotu są powiązane zgodnie z art. 60. Zasady techniczne niezbędne do wpisywania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w niniejszym ustępie, określa się i opracowuje w drodze środków wykonawczych zgodnie z procedurą sprawdzającą, o której mowa w art. 72 ust. 2.

Artykuł 33

Wykonanie działań na podstawie wpisu

1. W przypadku odnalezienia osoby, o której mowa w art. 32, właściwe organy powiadamiają, z zastrzeżeniem ust. 2, państwo członkowskie, które dokonało wpisu, o miejscu pobytu tej osoby. W przypadku dzieci zaginionych lub dzieci, które należy objąć ochroną, państwo członkowskie wykonujące wpis natychmiast porozumiewa się z państwem członkowskim dokonującym wpisu w celu niezwłocznego uzgodnienia środków, które należy podjąć w celu zabezpieczenia najlepszego interesu dziecka. W przypadkach, o których mowa w art. 32 ust. 2 lit. a) i c),

⁷⁴ Rozporządzenie Rady (WE) nr 2201/2003 z dnia 27 listopada 2003 r. dotyczące jurysdykcji oraz uznawania i wykonywania orzeczeń w sprawach małżeńskich oraz w sprawach dotyczących odpowiedzialności rodzicielskiej, uchylające rozporządzenie (WE) nr 1347/2000 (Dz.U. L 338 z 23.12.2003, s. 1).

właściwe organy mogą umieścić tę osobę w bezpiecznym miejscu, aby uniemożliwić jej kontynuowanie podróży, jeżeli uprawnia je do tego prawo krajowe.

2. Dane odnalezionej pełnoletniej osoby zaginionej mogą być przekazywane między jednostkami innymi niż właściwe organy tylko za zgodą tej osoby. Właściwe organy mogą jednak przekazać informacje o usunięciu wpisu z powodu odnalezienia zaginionej osoby zainteresowanemu, który zgłosił jej zaginięcie.

ROZDZIAŁ VIII

WPISY DOTYCZĄCE OSÓB, KTÓRYCH OBECNOŚĆ JEST WYMAGANA DO CELÓW PROCEDURY SĄDOWEJ

Artykuł 34

Cele i warunki dokonywania wpisów

1. Aby zapewnić informację o miejscu zamieszkania lub pobytu osób, państwa członkowskie wprowadzają do SIS na wniosek właściwego organu dane dotyczące:
 - a) świadków;
 - b) osób wezwanych do stawienia się przed organami sądowymi w związku z postępowaniem karnym lub w tym celu poszukiwanych, aby złożyły wyjaśnienia w sprawie czynów, za które są ścigane;
 - c) osób, którym ma zostać doręczony wyrok sądowy lub inne dokumenty związane z postępowaniem karnym, po to by złożyły wyjaśnienia w sprawie czynów, za które są ścigane;
 - d) osób, którym ma zostać doręczone wezwanie do stawienia się w celu odbycia kary pozbawienia wolności.
2. W przypadku gdy istnieje wyraźne wskazanie, że pojazdy, jednostka pływająca lub statki powietrzne są powiązane z osobą, której dotyczy wpis wydany zgodnie z ust. 1, wydane mogą zostać wpisy dotyczące tych pojazdów, łodzi i statków powietrznych w celu zlokalizowania tej osoby. W takich przypadkach wpisy dotyczące osoby oraz wpis dotyczący przedmiotu są powiązane zgodnie z art. 60. Zasady techniczne niezbędne do wpisywania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w niniejszym ustępie, określa się i opracowuje w drodze środków wykonawczych zgodnie z procedurą sprawdzającą, o której mowa w art. 72 ust. 2.

Artykuł 35

Wykonanie działania na podstawie wpisu

Wymagane informacje są przekazywane w drodze wymiany informacji uzupełniających państwu członkowskiemu, które o nie wystąpiło.

ROZDZIAŁ IX

WPISY DOTYCZĄCE OSÓB I PRZEDMIOTÓW WPROWADZANE W CELU PRZEPROWADZANIA KONTROLI NIEJAWNYCH, ROZPYTAŃ KONTROLNYCH LUB KONTROLI SZCZEGÓLNYCH

Artykuł 36

Cele i warunki dokonywania wpisów

1. Dane dotyczące osób lub pojazdów, jednostek pływających, statków powietrznych i kontenerów są wprowadzane zgodnie z prawem krajowym państwa członkowskiego, które dokonuje wpisu, do celów kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych zgodnie z art. 37 ust. 4.
2. Wpisu można dokonać w celu ścigania przestępstw, wykonania wyroku w sprawach karnych oraz zapobiegania zagrożeniom bezpieczeństwa publicznego:
 - a) jeżeli istnieją wyraźne oznaki, że dana osoba ma zamiar popełnić lub popełnia poważne przestępstwo, w szczególności przestępstwa, o których mowa w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW;
 - b) jeżeli informacje, o których mowa w art. 37 ust. 1, są konieczne do wykonania wyroku w sprawach karnych na osobie skazanej za popełnienie poważnego przestępstwa, w szczególności przestępstwa, o którym mowa w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW; lub
 - c) jeżeli ogólna ocena danej osoby, zwłaszcza w świetle wcześniej popełnionych przestępstw, daje powód do przypuszczenia, że osoba ta może popełniać poważne przestępstwa również w przyszłości, w szczególności przestępstwa, o których mowa w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW.
3. Ponadto wpisu można dokonać zgodnie z prawem krajowym na wniosek organów odpowiedzialnych za bezpieczeństwo narodowe, jeżeli istnieją konkretne przesłanki wskazujące, że informacje określone w art. 37 ust. 1 są niezbędne do zapobieżenia poważnemu zagrożeniu stwarzanemu przez daną osobę lub innym poważnym zagrożeniom wewnętrznego i zewnętrznego bezpieczeństwa narodowego. Państwo członkowskie dokonujące wpisu zgodnie z niniejszym ustępem powiadamia o tym pozostałe państwa członkowskie. Każde państwo członkowskie określa, którym organom przekazywane są takie informacje.
4. Jeżeli istnieją wyraźne oznaki, że pojazdy, jednostki pływające, statki powietrzne i kontenery są związane z poważnymi przestępstwami, o których mowa w ust. 2, lub z poważnymi zagrożeniami, o których mowa w ust. 3, można dokonać wpisów dotyczących tych pojazdów, jednostek pływających, statków powietrznych i kontenerów.
5. Jeżeli istnieją wyraźne oznaki, że blankiety dokumentów urzędowych lub wydane dokumenty tożsamości są związane z poważnymi przestępstwami, o których mowa w ust. 2, lub z poważnymi zagrożeniami, o których mowa w ust. 3, można dokonać wpisów dotyczących tych dokumentów niezależnie od tożsamości pierwotnego posiadacza tych dokumentów, jeżeli takowy istnieje. Techniczne zasady wpisywania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w niniejszym ustępie, określa się i opracowuje w drodze środków wykonawczych zgodnie z procedurą sprawdzającą, o której mowa w art. 72 ust. 2.

Artykuł 37

Wykonanie działania na podstawie wpisu

1. W celu przeprowadzania kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych wszystkie lub niektóre z poniższych informacji są gromadzone i przekazywane organowi dokonującemu wpisu, gdy na obszarze państwa członkowskiego prowadzone są kontrole graniczne, policyjne i celne lub wykonywane są inne czynności z zakresu ścigania przestępstw:
 - a) fakt odnalezienia osoby lub pojazdu, jednostki pływającej, statku powietrznego, kontenera, blankietu dokumentu urzędowego lub wydanego dokumentu tożsamości, których dotyczy wpis;
 - b) miejsce, godzina i przyczyna kontroli;
 - c) trasa i cel podróży;
 - d) osoby towarzyszące danej osobie lub osoby przewożone pojazdem, jednostką pływającą lub statkiem powietrznym, lub osoby towarzyszące osobie posiadającej blankiet dokumentu urzędowego lub wydany dokument tożsamości, co do których istnieją uzasadnione podejrzenia, że pozostają one w związku z osobami, których dotyczy wpis;
 - e) ujawniona tożsamość i opis osoby korzystającej z blankietu dokumentu urzędowego lub wydanego dokumentu tożsamości będących przedmiotem wpisu;
 - f) pojazd, jednostka pływająca, statek powietrzny lub kontener;
 - g) przewożone przedmioty, w tym dokumenty podróży;
 - h) okoliczności, w jakich osoba lub pojazd, jednostka pływająca, statek powietrzny, kontener, blankiety dokumentów urzędowych lub wydany dokument tożsamości zostały znalezione.
2. Informacje, o których mowa w ust. 1, są przekazywane w ramach wymiany informacji uzupełniających.
3. W zależności od okoliczności operacyjnych i zgodnie z prawem krajowym kontrola niejawna obejmuje kontrolę rutynową osoby lub przedmiotu w celu zgromadzenia jak największej ilości informacji wymienionych w ust. 1 bez zagrożenia dla niejawnego charakteru prowadzonej kontroli.
4. W zależności od okoliczności operacyjnych i zgodnie z prawem krajowym rozpytanie kontrolne obejmuje bardziej dogłębną kontrolę i przesłuchanie danej osoby. Jeżeli rozpytania kontrolne nie są dopuszczalne w świetle prawa państwa członkowskiego, są one zastępowane w tym państwie członkowskim kontrolami niejawnymi.
5. Podczas kontroli szczególnych osoby, pojazdy, jednostki pływające, statki powietrzne, kontenery oraz przewożone przedmioty mogą zostać przeszukane zgodnie z prawem krajowym w celach, o których mowa w art. 36. Wyszukiwania przeprowadza się zgodnie z prawem krajowym. Jeżeli kontrole szczególne nie są dopuszczalne w świetle prawa państwa członkowskiego, są one zastępowane w tym państwie członkowskim rozpytaniami kontrolnymi.

ROZDZIAŁ X

WPISY DOTYCZĄCE PRZEDMIOTÓW PRZEZNACZONYCH DO ZAJĘCIA LUB WYKORZYSTANIA JAKO DOWÓD W POSTĘPOWANIU KARNYM

Artykuł 38

Cele i warunki dokonywania wpisów

1. Dane dotyczące przedmiotów poszukiwanych w celu ich zajęcia na użytek ścigania przestępstw lub wykorzystania jako dowód w postępowaniu karnym są wprowadzane do SIS.
2. Wprowadza się następujące kategorie łatwych do zidentyfikowania przedmiotów:
 - a) pojazdy silnikowe zdefiniowane w prawie krajowym, niezależnie od układu napędowego;
 - b) przyczepy o masie własnej przekraczającej 750 kg;
 - c) przyczepy turystyczne;
 - d) urządzenia przemysłowe;
 - e) jednostki pływające;
 - f) silniki do łodzi;
 - g) kontenery;
 - h) statki powietrzne;
 - i) broń palna;
 - j) blankiety dokumentów urzędowych, które zostały skradzione, przywłaszczone lub utracone;
 - k) wydane dokumenty tożsamości, takie jak paszporty, dowody tożsamości, prawa jazdy, dokumenty pobytowe i dokumenty podróży, które zostały skradzione, przywłaszczone, utracone lub unieważnione lub które mają charakter takich dokumentów, lecz zostały sfalszowane;
 - l) skradzione, przywłaszczone, zaginione lub unieważnione dowody i tablice rejestracyjne pojazdów lub dowody i tablice rejestracyjne pojazdów, które mają charakter takich dokumentów i tablic rejestracyjnych, lecz zostały sfalszowane;
 - m) banknoty (o spisanych numerach) i banknoty sfalszowane;
 - n) wyposażenie techniczne, sprzęt informatyczny i inne możliwe do zidentyfikowania przedmioty o wysokiej wartości;
 - o) możliwe do zidentyfikowania części pojazdów silnikowych;
 - p) możliwe do zidentyfikowania części urządzeń przemysłowych.
3. Definicje nowych podkategorii przedmiotów wymienionych w ust. 2 lit. n) oraz 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. 72 ust. 2.

Artykuł 39

Wykonanie działania na podstawie wpisu

1. Jeżeli wyszukiwanie w systemie wykaże istnienie wpisu dotyczącego przedmiotu, który został znaleziony, organ, który stwierdził zgodność wpisu z przedmiotem, zgodnie z prawem krajowym zajmuje ten przedmiot i zgłasza ten fakt organowi, który dokonał wpisu, tak by ustalić konieczne działania. W tym celu dopuszcza się także przekazywanie danych osobowych zgodnie z niniejszym rozporządzeniem.
2. Informacje, o których mowa w ust. 1, są przekazywane w ramach wymiany informacji uzupełniających.
3. Państwo członkowskie, które odnalazło dany przedmiot, podejmuje działania, o które wnioskowano, zgodnie z prawem krajowym.

ROZDZIAŁ XI

WPISY DOTYCZĄCE NIEZNANYCH OSÓB POSZUKIWANYCH NA POTRZEBY IDENTYFIKACJI ZGODNIE Z PRAWEM KRAJOWYM I WYSZUKIWANIE ZA POMOCĄ DANYCH BIOMETRYCZNYCH

Artykuł 40

Wpisy dotyczące nieznanych osób poszukiwanych na potrzeby zatrzymania zgodnie z prawem krajowym

Do SIS można wprowadzać dane daktyloskopijne, które nie dotyczą osób będących przedmiotem wpisu. Wspomniane dane daktyloskopijne muszą być kompletnymi lub niekompletnymi zestawami linii papilarnych lub odcisków dłoni znalezionych na miejscu przestępstwa będącego przedmiotem dochodzenia, poważnego przestępstwa lub przestępstwa terrorystycznego oraz z dużym prawdopodobieństwem można stwierdzić, że należą one do sprawcy przestępstwa. Dane daktyloskopijne należące do tej kategorii przechowywane są w zbiorze „sprawca nieznany lub osoba poszukiwana”, pod warunkiem że właściwe organy nie mogą ustalić tożsamości osoby przy użyciu jakiegokolwiek innej krajowej, europejskiej lub międzynarodowej bazy danych.

Artykuł 41

Wykonanie działania na podstawie wpisu

W przypadku trafienia lub potencjalnego dopasowania do danych przechowywanych zgodnie z art. 40 tożsamość osoby określa się zgodnie z prawem krajowym, weryfikując, czy dane daktyloskopijne przechowywane w SIS należą do danej osoby. Państwa członkowskie porozumiewają się przy użyciu informacji uzupełniających w celu ułatwienia przeprowadzenia terminowego dochodzenia w danej sprawie.

Artykuł 42

Zasady szczegółowe dotyczące weryfikacji lub wyszukiwania fotografii, obrazów twarzy, danych daktyloskopijnych i profili DNA

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

2. Dane daktyloskopijne można wykorzystać również do zidentyfikowania danej osoby. Dane daktyloskopijne przechowywane w SIS wyszukuje 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. 26, 34 ust. 1 lit. b) i d) oraz art. 36 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 jakiegokolwiek 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 XII

PRAWO DO DOSTĘPU I PRZECHOWYWANIE WPISÓW

Artykuł 43

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:
 - a) kontrolę graniczną 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) kontrole policyjne i celne prowadzone na terytorium danego państwa członkowskiego oraz koordynację takich kontroli przez wyznaczone organy;
 - c) inne czynności z zakresu ścigania przestępstw wykonywane w celu zapobiegania przestępstwom, wykrywania przestępstw i prowadzenia dochodzeń dotyczących przestępstw w danym państwie członkowskim;
 - d) badanie warunków i podejmowanie 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.
2. 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 podstawie 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. Z prawa do dostępu do danych wprowadzonych do SIS oraz do bezpośredniego wyszukiwania takich danych mogą korzystać organy właściwe do wykonywania zadań, o których mowa w ust. 1 lit. c), na potrzeby wykonywania tych zadań. Dostęp tych organów jest regulowany prawem każdego z państw członkowskich.
4. Organy, o których mowa w niniejszym artykule, są uwzględniane w wykazie, o którym mowa w art. 53 ust. 8.

Artykuł 44 *Organy rejestrujące pojazdy*

1. Służby państw członkowskich odpowiedzialne za wydawanie dowodów rejestracyjnych pojazdów, o których mowa w dyrektywie Rady 1999/37/WE⁷⁵, posiadają dostęp do następujących danych wprowadzonych do SIS zgodnie z art. 38 ust. 2 lit. a), b), c) i l) niniejszego rozporządzenia wyłącznie na potrzeby sprawdzenia, czy pojazdy, o których rejestrację zwrócono się do tych organów, zostały skradzione, przywłaszczone lub zagubione lub czy są poszukiwane jako dowód w postępowaniu karnym:
 - a) dane dotyczące pojazdów silnikowych zdefiniowanych w prawie krajowym, niezależnie od układu napędowego;
 - b) dane dotyczące przyczep o masie własnej przekraczającej 750 kg i przyczep turystycznych;
 - c) dane dotyczące dowodów rejestracyjnych oraz tablic rejestracyjnych pojazdów, które zostały skradzione, przywłaszczone, utracone lub unieważnione.Dostęp do tych danych przez służby odpowiedzialne za wydawanie dowodów rejestracyjnych pojazdów jest regulowany prawem krajowym danego państwa członkowskiego.
2. Służby, o których mowa w ust. 1, będące służbami rządowymi, mają prawo do bezpośredniego dostępu do danych wprowadzonych do SIS.
3. Służby, o których mowa w ust. 1, niebędące służbami rządowymi, mają dostęp do danych wprowadzonych do SIS wyłącznie za pośrednictwem organu, o którym mowa w art. 43 niniejszego rozporządzenia. Organ ten ma prawo do bezpośredniego dostępu do tych danych i przekazywania ich zainteresowanym służbom. Zainteresowane państwo członkowskie zapewnia, by przedmiotowe służby i ich pracownicy byli zobowiązani do przestrzegania wszelkich ograniczeń dotyczących dozwolonego wykorzystywania danych przekazywanych im przez ten organ.
4. Artykuł 39 niniejszego rozporządzenia nie ma zastosowania do dostępu uzyskanego zgodnie z niniejszym artykułem. Prawo krajowe reguluje przekazywanie policji lub organom sądowiczym przez służby, o których mowa w ust. 1, informacji ujawnionych w wyniku dostępu do SIS i stanowiących podstawę do podejrzeń, że popełnione zostało przestępstwo.

⁷⁵ Dyrektywa Rady 1999/37/WE z dnia 29 kwietnia 1999 r. w sprawie dokumentów rejestracyjnych pojazdów (Dz.U. L 138 z 1.6.1999, s. 57).

Artykuł 45

Organy rejestrujące jednostki pływające i statki powietrzne

1. Służby państw członkowskich odpowiedzialne za wydawanie dowodów rejestracyjnych lub za zapewnianie zarządzania ruchem w odniesieniu do jednostek pływających, w tym silników do łodzi, i statków powietrznych posiadają dostęp do następujących danych wprowadzonych do SIS zgodnie z art. 38 ust. 2 niniejszego rozporządzenia wyłącznie na potrzeby sprawdzenia, czy jednostki pływające, w tym silniki do łodzi, statki powietrzne lub kontenery, o których rejestrację zwrócono się do tych organów lub które podlegają zarządzaniu ruchem, zostały skradzione, przywłaszczone lub zagubione lub czy są poszukiwane jako dowód w postępowaniu karnym:
 - a) dane dotyczące jednostek pływających;
 - b) dane dotyczące silników do łodzi;
 - c) dane dotyczące statków powietrznych.

Z zastrzeżeniem ust. 2 dostęp powyższych służb w danym państwie członkowskim do tych danych reguluje prawo każdego państwa członkowskiego. Dostęp do danych wymienionych w lit. a)–c) powyżej jest ograniczony do specjalnej właściwości danych służb.

2. Służby, o których mowa w ust. 1, będące służbami rządowymi, mają prawo do bezpośredniego dostępu do danych wprowadzonych do SIS.
3. Służby, o których mowa w ust. 1, niebędące służbami rządowymi, mają dostęp do danych wprowadzonych do SIS wyłącznie za pośrednictwem organu, o którym mowa w art. 43 niniejszego rozporządzenia. Organ ten ma prawo do bezpośredniego dostępu do danych i przekazywania ich zainteresowanym służbom. Zainteresowane państwo członkowskie zapewnia, by służby te i ich pracownicy byli zobowiązani do przestrzegania wszelkich ograniczeń dotyczących dozwolonego wykorzystywania danych przekazywanych im przez ten organ.
4. Artykuł 39 niniejszego rozporządzenia nie ma zastosowania do dostępu uzyskanego zgodnie z niniejszym artykułem. Prawo krajowe reguluje przekazywanie policji lub organom sądowym przez służby, o których mowa w ust. 1, informacji ujawnionych w wyniku dostępu do SIS i stanowiących podstawę do podejrzeń, że popełnione zostało przestępstwo.

Artykuł 46

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 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 jakiegokolwiek części SIS.

Artykuł 47
Dostęp do danych SIS przez Eurojust

1. Krajowi przedstawiciele oddelegowani do Eurojustu oraz ich asystenci w ramach swojego mandatu mają prawo do dostępu do danych wprowadzonych do SIS zgodnie z art. 26, 32, 34, 38 i 40 oraz do wyszukiwania tych danych w ramach swojego mandatu.
2. Jeżeli podczas wyszukiwania danych oddelegowany do Eurojustu krajowy przedstawiciel stwierdzi istnienie wpisu w SIS, informuje o tym państwo członkowskie dokonujące wpisu.
3. Przepisy niniejszego artykułu nie mogą być interpretowane jako modyfikacja przepisów decyzji 2002/187/WSiSW dotyczących ochrony danych i odpowiedzialności prawnej za wszelkie nieuprawnione lub nieprawidłowe przetwarzanie takich danych przez krajowych przedstawicieli oddelegowanych do Eurojustu lub ich asystentów, ani też jako modyfikacja uprawnień wspólnego organu nadzorczego, ustanowionego na mocy tej decyzji.
4. Każdy przypadek uzyskania dostępu i przeprowadzenia wyszukiwania przez krajowego przedstawiciela oddelegowanego do Eurojustu lub jego asystenta zostaje zarejestrowany zgodnie z przepisami art. 12; rejestracji podlega również każde wykorzystanie przez nich danych, do których uzyskali dostęp.
5. Żadnych części SIS nie podłącza się do jakiegokolwiek systemu komputerowego służącego do gromadzenia i przetwarzania danych obsługiwanego przez Eurojust lub w siedzibie Eurojustu, a danych zawartych w SIS, udostępnianych krajowym przedstawicielom i ich asystentom, nie przesyła się do jakiegokolwiek takiego systemu komputerowego. Nie można pobierać żadnych części SIS. Rejestrowania przypadków dostępu i wyszukiwania nie należy interpretować jako niezgodnego z prawem pobierania lub kopiowania danych SIS.
6. Dostęp do danych wprowadzonych do SIS jest zastrzeżony dla krajowych przedstawicieli i ich asystentów i nie może być rozszerzony na pracowników Eurojustu.
7. Przyjmowane i stosowane są środki mające na celu zapewnienie bezpieczeństwa i poufności przewidziane w art. 10 i 11.

Artykuł 48
Dostęp zespołów Europejskiej Straży Granicznej i Przybrzeżnej, zespołów składających się z personelu realizującego zadania w dziedzinie powrotów oraz członków zespołu wspierającego 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. 49 ust. 1.

3. Jeżeli podczas wyszukiwania członek zespołów Europejskiej Straży Granicznej i Przybrzeżnej, zespołów składających się z personelu realizującego zadania w dziedzinie powrotów lub zespołu wspierającego 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 zespołu wspierającego 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 zespołu wspierającego 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 49

Dostęp Europejskiej Agencji Straży Granicznej i Przybrzeżnej do danych SIS

1. Do celów art. 48 ust. 1 i ust. 2 niniejszego artykułu Europejska Agencja Straży Granicznej i Przybrzeżnej ustanawia i prowadzi interfejs techniczny, który umożliwia bezpośrednie połączenie z centralnym SIS.
2. 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 i wyszukiwania danych wprowadzonych do SIS zgodnie z art. 26, 32, 34, 36 i art. 38 ust. 2 lit. j) i k).
3. Jeżeli podczas weryfikacji 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).
4. 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.

5. Każdy przypadek uzyskania dostępu i przeprowadzenia wyszukiwania przez Europejską Agencję Straży Granicznej i Przybrzeżnej zostaje zarejestrowany zgodnie z art. 12; rejestracji podlega również każde wykorzystanie przez nich danych, do których uzyskali dostęp.
6. 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 obsługiwane 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.
7. Europejska Agencja Straży Granicznej i Przybrzeżnej przyjmuje i stosuje środki mające na celu zapewnienie bezpieczeństwa i poufności przewidziane w art. 10 i 11.

Artykuł 50
Zakres dostępu

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

Artykuł 51
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. Wpisy dokonane do celów art. 36 niniejszego rozporządzenia przechowuje się maksymalnie przez okres jednego roku.
3. Wpisy dotyczące blankietów dokumentów urzędowych i wydanych dokumentów tożsamości wprowadzone zgodnie z art. 38 przechowywane są maksymalnie przez okres dziesięciu lat. Krótsze okresy przechowywania w odniesieniu do kategorii wpisów dotyczących przedmiotów można określić w drodze środków wykonawczych przyjętych zgodnie z procedurą sprawdzającą określoną w art. 72 ust. 2.
4. Każde państwo członkowskie ustanawia w stosownych przypadkach krótsze terminy weryfikacji, zgodnie ze swoim prawem krajowym.
5. 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 rozagę. 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 nadzorcemu.

6. 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.
7. 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 zgodnie z ust. 6. CS-SIS automatycznie informuje państwa członkowskie z czteromiesięcznym wyprzedzeniem o zaplanowanym usunięciu danych z systemu.
8. Państwa członkowskie przechowują statystyki dotyczące liczby wpisów, których okres przechowywania został przedłużony zgodnie z ust. 6.

ROZDZIAŁ XIII

USUWANIE WPISÓW

Artykuł 52

Usuwanie wpisów

1. Wpisy mające doprowadzić do aresztowania i wydania lub ekstradycji zgodnie z art. 26 usuwa się po wydaniu lub ekstradycji danej osoby właściwym organom państwa członkowskiego dokonującego wpisu. Wpisy można również usunąć w przypadku uchylenia decyzji stanowiącej podstawę wpisu przez właściwy według prawa krajowego organ sądowy.
2. Wpisy dotyczące osób zaginionych usuwa się zgodnie z następującymi zasadami:
 - a) w przypadku dzieci zaginionych, zgodnie z art. 32, wpis usuwa się w następstwie:
 - rozwiązania sprawy, np. gdy dziecko zostało poddane repatriacji lub gdy właściwe organy w państwie członkowskim wykonującym wpis podjęły decyzję dotyczącą opieki nad dzieckiem;
 - wygaśnięcia wpisu zgodnie z art. 51;
 - decyzji właściwego organu państwa członkowskiego dokonującego wpisu, lub
 - odnalezienia dziecka;
 - b) w przypadku zaginionych osób dorosłych, zgodnie z art. 32 – jeżeli nie wystąpiono o żadne środki ochrony – wpis usuwa się w następstwie:
 - realizacji niezbędnych działań (ustalenia miejsca pobytu przez państwo członkowskie wykonujące wpis);

- wygaśnięcia wpisu zgodnie z art. 51; lub
 - decyzji właściwego organu państwa członkowskiego dokonującego wpisu;
- c) w przypadku zaginionych osób dorosłych, zgodnie z art. 32 – jeżeli wystąpiono o środki ochrony – wpis usuwa się w następstwie:
- przeprowadzenia niezbędnego działania (objęcie osoby ochroną);
 - wygaśnięcia wpisu zgodnie z art. 51; lub
 - decyzji właściwego organu państwa członkowskiego dokonującego wpisu.

Z zastrzeżeniem prawa krajowego, jeżeli osoba została internowana w następstwie decyzji podjętej przez właściwy organ, wpis można przechować do czasu repatriacji tej osoby.

3. Wpisy dotyczące osób poszukiwanych do celów procedury sądowej usuwa się zgodnie z następującymi zasadami:

w przypadku wpisów dotyczących osób poszukiwanych do celów procedury sądowej, zgodnie z art. 34, wpis usuwa się w następstwie:

- a) przekazania informacji o miejscu pobytu osoby właściwemu organowi państwa członkowskiego dokonującego wpisu. Jeżeli nie można podjąć działań w związku z przekazanymi informacjami, biuro SIRENE państwa członkowskiego dokonującego wpisu powiadamia biuro SIRENE państwa członkowskiego wykonującego wpis w celu rozwiązania problemu;
- b) wygaśnięcia wpisu zgodnie z art. 51; lub
- c) decyzji właściwego organu państwa członkowskiego dokonującego wpisu.

W przypadku gdy uzyskano trafienie w państwie członkowskim i dane adresowe zostały przekazane państwu członkowskiemu dokonującemu wpisu, a kolejne trafienie w tym państwie członkowskim wskazuje te same dane adresowe, trafienie rejestruje się w państwie członkowskim wykonującym wpis, przy czym do państwa członkowskiego dokonującego wpisu nie przesyła się ponownie ani danych adresowych, ani informacji uzupełniających. W takich przypadkach państwo członkowskie wykonujące wpis informuje państwo członkowskie dokonujące wpisu o powtarzających się trafieniach, a państwo członkowskie dokonujące wpisu rozważy konieczność utrzymania wpisu.

4. Wpisy dotyczące kontroli niejawnych, rozpytań kontrolnych i kontroli szczególnych usuwa się zgodnie z następującymi zasadami:

w przypadku wpisów dotyczących kontroli niejawnych, rozpytań kontrolnych i kontroli szczególnych, zgodnie z art. 36, wpis usuwa się w następstwie:

- a) wygaśnięcia wpisu zgodnie z art. 51;
- b) decyzji o usunięciu podjętej przez właściwy organ państwa członkowskiego dokonującego wpisu.

5. Wpisy dotyczące przedmiotów przeznaczonych do zajęcia lub wykorzystania jako dowód usuwa się zgodnie z następującymi zasadami:

w przypadku wpisów dotyczących przedmiotów przeznaczonych do zajęcia lub wykorzystania jako dowód w postępowaniu karnym, zgodnie z art. 38, wpis usuwa się w następstwie:

- a) zajęcia przedmiotu lub podjęcia równoważnego środka po przeprowadzeniu koniecznych działań następczych w zakresie wymiany informacji uzupełniających między biurami SIRENE lub po tym, jak przedmiot zostanie objęty innym postępowaniem sądowym lub administracyjnym;
 - b) wygaśnięcia wpisu; lub
 - c) decyzji o usunięciu podjętej przez właściwy organ państwa członkowskiego dokonującego wpisu.
6. Wpisy dotyczące nieznanymi osób poszukiwanych zgodnie z art. 40 usuwa się zgodnie z następującymi zasadami:
7. a) po zidentyfikowaniu osoby; lub
8. b) po wygaśnięciu wpisu.

ROZDZIAŁ XIV

OGÓLNE ZASADY PRZETWARZANIA DANYCH

Artykuł 53

Przetwarzanie danych SIS

1. Państwa członkowskie mogą przetwarzać dane określone w art. 20 wyłącznie w celach, jakie zostały określone dla każdej z kategorii wpisów, o których mowa w art. 26, 32, 34, 36, 38 i 40.
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. 43. 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.
4. 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.
5. Prawo dostępu do danych przyznaje się wyłącznie w granicach kompetencji organów krajowych, o których mowa w art. 43, właściwie upoważnionym pracownikom.
6. W odniesieniu do wpisów, o których mowa w art. 26, 32, 34, 36, 38 i 40 niniejszego rozporządzenia, każdy przypadek przetwarzania zawartych w nich 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.

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 54

Dane SIS a pliki krajowe

1. Artykuł 53 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 53 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 55

Informacja w przypadku niewykonania wpisu

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

Artykuł 56

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. 59.
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 57

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 powiadamiają Komisję, Agencję i krajowy organ nadzorczy o incydentach związanych z bezpieczeństwem informacji. 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 przekazaniem przez Agencję planem zarządzania incydentami.

Artykuł 58

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. 56 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 59

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) fotografie i wizerunki 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. 72 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 60

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, o której mowa w art. 72 ust. 2.

Artykuł 61

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 same dokonały, lub wpisów, w związku z którymi podjęto działania na jego terytorium. Okres przechowywania takich danych we wspomnianych plikach reguluje prawo krajowe.

Artykuł 62
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.

Artykuł 63
Wymiana z Interpolem danych na temat skradzionych, przywłaszczonych, utraconych lub unieważnionych paszportów

1. W drodze odstępstwa od art. 62 wprowadzone do SIS informacje o numerze, kraju wystawienia i typie paszportów skradzionych, przywłaszczonych, utraconych lub unieważnionych mogą być wymieniane z członkami Interpolu poprzez ustanowienie połączenia pomiędzy SIS a bazą Interpolu zawierającą dane skradzionych lub utraconych dokumentów podróży, o ile zostanie zawarta umowa między Interpolem a Unią Europejską. Umowa ta musi zawierać zastrzeżenie, że przekazanie danych wprowadzonych przez dane państwo członkowskie zależy od zgody tego państwa członkowskiego.
2. Umowa, o której mowa w ust. 1, przewiduje, że wymieniane dane są dostępne wyłącznie dla członków Interpolu z państw, które zapewniają odpowiedni poziom ochrony danych osobowych. Przed zawarciem tej umowy Rada zasięga opinii Komisji co do adekwatności poziomu ochrony danych osobowych oraz poszanowania podstawowych praw i wolności w odniesieniu do automatycznego przetwarzania danych osobowych przez Interpol i przez państwa, które oddelegowały swoich przedstawicieli do Interpolu.
3. Umowa, o której mowa w ust. 1, może także przewidywać dostęp państw członkowskich za pośrednictwem SIS do danych z bazy Interpolu zawierającej dane skradzionych lub utraconych dokumentów podróży, zgodnie z odpowiednimi przepisami niniejszej decyzji dotyczącymi wpisów do SIS na temat skradzionych, przywłaszczonych, utraconych lub unieważnionych paszportów.

ROZDZIAŁ XV

OCHRONA DANYCH

Artykuł 64
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 (UE) 2016/679 stosuje się w odniesieniu do przetwarzania danych osobowych, 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 65

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 należyтым 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. Każdy ma prawo do żądania, by dotyczące go dane niezgodne ze stanem faktycznym zostały poprawione, a dotyczące go dane przechowywane z naruszeniem prawa usunięte.
6. 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.
7. 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 66
Środki odwoławcze

1. Każdy może wystąpić do sądów lub organów właściwych na mocy prawa krajowego któregośkolwiek z państw członkowskich z wnioskiem o dostęp do informacji, poprawienie, usunięcie lub uzyskanie 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. 70.
3. Aby uzyskać spójny przegląd funkcjonowania środków odwoławczych, organy krajowe opracowują standardowy system statystyczny 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. 69.

Artykuł 67
Nadzór nad N.SIS

1. Każde państwo członkowskie zapewnia, by krajowy organ nadzorczy lub 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 krajowy organ nadzorczy 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 68 *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 69 *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 XVI

ODPOWIEDZIALNOŚĆ

Artykuł 70 *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 rozmiar.

ROZDZIAŁ XVII

PRZEPISY KOŃCOWE

Artykuł 71 *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 sporządzaienne, miesięczne i roczne statystyki pokazujące liczbę rekordów przypadających na daną kategorię wpisów, liczbę uzyskanych rocznie w systemie 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. Statystyki te nie zawierają żadnych danych osobowych. Roczne sprawozdanie statystyczne podlega publikacji. Agencja dostarcza również roczne statystyki dotyczące korzystania z funkcji polegającej na czasowym uniemożliwieniu wyszukiwania wpisu dokonanego

zgodnie z art. 26 niniejszego rozporządzenia ogółem oraz w rozbiciu na poszczególne państwa członkowskie, w tym wszelkich przypadków przedłużenia 48-godzinnego okresu tymczasowego ograniczenia dostępu.

4. Państwa członkowskie oraz Europol, Eurojust i Europejska Agencja Straży Granicznej i Przybrzeżnej przekazują Agencji i Komisji informacje niezbędne do sporządzenia sprawozdań, o których mowa w ust. 3, 7 i 8. Informacje te obejmują odrębne dane statystyczne dotyczące liczby wyszukiwań prowadzonych przez służby państw członkowskich odpowiedzialne za wydawanie dowodów rejestracyjnych pojazdów oraz służby państw członkowskich odpowiedzialne za wydawanie dowodów rejestracyjnych lub za zarządzanie ruchem jednostek pływających, w tym silników do łodzi, statków powietrznych oraz kontenerów, lub w imieniu tych służb. Wspomniane dane statystyczne pokazują również liczbę trafień uzyskanych w systemie przypadających na daną kategorię wpisów.
5. Agencja przekazuje państwom członkowskim, Komisji, Europolowi, Eurojustowi 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, 4 i 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, Eurojustowi 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 przyjmuje się w drodze środków wykonawczych przyjętych zgodnie z procedurą sprawdzającą, o której mowa w art. 72 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 72
Procedura komitetowa

1. Komisja jest wspierana przez komitet w rozumieniu rozporządzenia (UE) nr 182/2011.
2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 73
Zmiany w rozporządzeniu (UE) nr 515/2014

W rozporządzeniu (UE) nr 515/2014⁷⁶ 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 74
Uchylenie

Wraz z dniem rozpoczęcia stosowania niniejszego rozporządzenia uchyla się następujące akty prawne:

rozporządzenie (WE) nr 1986/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie dostępu służb odpowiedzialnych w państwach członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji (SIS II);

decyzję Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II);

decyzję Komisji 2010/261/UE z dnia 4 maja 2010 r. w sprawie planu bezpieczeństwa dla centralnego systemu SIS II i infrastruktury łączności⁷⁷.

⁷⁶ 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).

⁷⁷ 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).

Artykuł 75
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;
 - 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
Przewodniczący

W imieniu Rady
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 współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmieniające rozporządzenie (UE) nr 515/2014 i uchylające rozporządzenie (WE) nr 1986/2006, decyzję Rady 2007/533/WSiSW i decyzję Komisji 2010/261/UE

1.2. Dziedziny polityki w strukturze ABM/ABB⁷⁸, których dotyczy wniosek/inicjatywa

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**⁷⁹
- ☒ 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 – „Walka z przestępczością zorganizowaną”

Cel – „Zdecydowana reakcja UE w celu przeciwdziałania terroryzmowi i zapobiegania radykalizacji”

Komisja wielokrotnie podkreślała konieczność zrewidowania podstawy prawnej SIS w celu podjęcia nowych wyzwań związanych z bezpieczeństwem i migracją. Przykładowo w „Europejskiej agendzie bezpieczeństwa”⁸⁰ Komisja wyraziła swój zamiar dokonania oceny SIS w latach 2015–2016, aby stwierdzić, czy nowe potrzeby operacyjne wymagają zmian legislacyjnych. Co więcej, w agendzie bezpieczeństwa podkreślono, że SIS stanowi kluczowy element policyjnej wymiany informacji i że system ten należy dalej usprawniać. Ostatnio w komunikacie „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa”⁸¹ Komisja stwierdziła, że dodatkowe funkcje systemu zostaną poddane pod rozwałę na podstawie sprawozdania z ogólnej oceny w celu przedstawienia wniosków w sprawie zmiany podstawy prawnej SIS. Następnie w komunikacie z dnia 20 kwietnia 2016 r. „Realizacja Europejskiej agendy

⁷⁸ ABM: *activity-based management*: zarządzanie kosztami działań; ABB: *activity-based budgeting*: budżet zadaniowy.

⁷⁹ O którym mowa w art. 54 ust. 2 lit. a) lub b) rozporządzenia finansowego.

⁸⁰ COM(2015) 185 final.

⁸¹ COM(2016) 205 final.

bezpieczeństwa w celu zwalczania terroryzmu i utorowania drogi ku rzeczywistej i skutecznej unii bezpieczeństwa”⁸² Komisja przedstawiła szereg zmian w SIS, aby zwiększyć wartość dodaną systemu na użytek ścigania przestępstw.

Ogólna ocena przeprowadzona przez Komisję potwierdziła, że SIS odniósł sukces operacyjny. Pomimo jego licznych zalet w ocenie zawarto jednak też szereg zaleceń w celu zwiększenia technicznej i operacyjnej efektywności i skuteczności systemu.

Na podstawie zaleceń sprawozdania z ogólnej oceny i z zachowaniem pełnej zgodności z celami Komisji wyrażonymi w wyżej wymienionych komunikatach i Planie Strategicznym na lata 2016–2020 DG ds. Migracji i Spraw Wewnętrznych⁸³ celem niniejszego wniosku jest wdrożenie:

- oświadczenia Komisji zapowiadającego zwiększenie wartości dodanej SIS na potrzeby ścigania przestępstw do celów reagowania na nowe zagrożenia;
- zaleceń dotyczących wprowadzenia technicznych i proceduralnych zmian w następstwie kompleksowej oceny SIS;
- usprawnień technicznych, o które wnioskowali użytkownicy końcowi SIS;
- wstępnych ustaleń dotyczących jakości danych sformułowanych przez grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności.

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 2.1 – Zdecydowana reakcja UE w celu przeciwdziałania terroryzmowi i zapobiegania radykalizacji

Cel szczegółowy 2.2 – Walka z poważną i zorganizowaną przestępczością transgraniczną

Działania ABM/ABB, których dotyczy wniosek/inicjatywa

Rozdział 18 02 – Bezpieczeństwo wewnętrzne

⁸² COM(2016) 230 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.

Podstawowym celem proponowanych zmian prawnych i technicznych w SIS jest podniesienie efektywności operacyjnej systemu. W wyniku ogólnej oceny SIS dokonanej przez DG HOME w latach 2015–2016 zalecono wprowadzenie usprawnień technicznych systemu i harmonizację krajowych procedur w dziedzinie współpracy organów ścigania.

W nowym wniosku wprowadzono środki, które stanowią odpowiedź na potrzeby operacyjne i techniczne użytkowników końcowych. W szczególności nowe pola danych dla obecnych wpisów umożliwią funkcjonariuszom policji 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 pracę funkcjonariuszy organów ścigania. Ponadto niniejszy wniosek obejmuje zmiany techniczne, które zwiększą skuteczność systemu i sprawią, że korzystanie z niego będzie łatwiejsze.

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.

Niniejszy wniosek wprowadza nowe identyfikatory biometryczne – odciski dłoni, wizerunki twarzy i profile DNA w ograniczonej liczbie konkretnych przypadków. Wszystko to wraz z planowanymi zmianami w art. 32 i 33 (wpisy dotyczące osób zaginionych), które mają umożliwić wprowadzanie wpisów przewencyjnych i kategoryzację przypadków osób zaginionych, po pierwsze w znacznym stopniu wzmocni ochronę małoletnich bez opieki, a po drugie pozwoli na ich identyfikację na podstawie profilu DNA małoletniego lub jego rodziców bądź rodzeństwa (za zgodą).

Organy państw członkowskich będą również mogły dokonywać wpisów dotyczących nieznanych osób fizycznych poszukiwanych w związku z popełnieniem przestępstwa na podstawie niewidocznych śladów linii papilarnych lub odcisków dłoni lub też śladów linii papilarnych lub odcisków dłoni pozyskanych w miejscu przestępstwa. W obecnych ramach prawnych i technicznych nie jest to możliwe, a zatem zmiana ta jest bardzo istotna.

1.4.4. *Wskaźniki wyników i wpływu*

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

W trakcie modernizacji systemu:

Po zatwierdzeniu wniosku i przyjęciu specyfikacji technicznych SIS zostanie poddany modernizacji w celu lepszej harmonizacji procedur krajowych na potrzeby użytkownika systemu, poszerzenia zakresu stosowania systemu przez wprowadzenie nowych elementów w obecnych kategoriach wpisów 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 w systemie 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. Ponadto Agencja będzie również publikować roczne statystyki dotyczące korzystania z funkcji polegającej na czasowym uniemożliwieniu wyszukiwania wpisu dokonanego zgodnie z art. 26 niniejszego rozporządzenia ogółem oraz w rozbiciu na poszczególne państwa członkowskie, w tym wszelkie przypadki przedłużenia 48-godzinnego okresu tymczasowego ograniczenia dostępu.

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.

Cel szczegółowy 1 – Walka z przestępczością zorganizowaną.

Wskaźnik – Wykorzystanie unijnych mechanizmów wymiany informacji. Można go zmierzyć dzięki wzrostowi liczby trafień w SIS. Jako wskaźniki służyć będą sprawozdania statystyczne sporządzane przez eu-LISA i państwa członkowskie. Umożliwi to Komisji dokonanie oceny sposobu korzystania z nowych funkcji systemu.

Cel szczegółowy 2 – Zdecydowana reakcja UE w celu przeciwdziałania terroryzmowi i zapobiegania radykalizacji.

Wskaźnik – Wzrost liczby wpisów i trafień, w szczególności w odniesieniu do art. 36 ust. 3 dotyczącego wpisów dotyczących osób i przedmiotów wprowadzanych w celu przeprowadzania kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych.

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. Lepsza harmonizacja procedur krajowych na potrzeby użytkowania SIS.
3. Poszerzenie wykazu użytkowników instytucjonalnych mających dostęp do danych SIS poprzez udzielenie pełnego dostępu do systemu Europolowi i nowej Europejskiej Straży Granicznej i Przybrzeżnej.
4. Wprowadzenie nowych elementów we wpisach SIS i nowych funkcji w celu poszerzenia zakresu stosowania systemu, umożliwienia jego działania w obecnym środowisku bezpieczeństwa, usprawnienia współpracy między organami ścigania i organami bezpieczeństwa państw członkowskich oraz ograniczenia obciążeń administracyjnych.
5. Uwzględnienie pełnego użytkowania całego SIS, w tym nie tylko samego funkcjonowania systemu centralnego i systemu krajowego, lecz także zapewnienie, aby użytkownicy końcowi otrzymywali wszystkie dane, które są im niezbędne do wykonywania powierzonych im zadań.
6. Zwiększenie ciągłości działania i zapewnienie niezakłóconego działania SIS na szczeblu centralnym i krajowym.
7. Wzmocnienie środków zwalczania przestępczości międzynarodowej, terroryzmu i cyberprzestępczości, czyli wzajemnie ze sobą powiązanych obszarów o silnie zarysowanym wymiarze transgranicznym.

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. 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. właściwe organy państw członkowskich korzystały z systemu blisko 2,9 mld razy, co w sposób oczywisty wskazuje na istotny wkład systemu we współpracę organów ścigania w strefie Schengen. Tak wysoki poziom wymiany

informacji między państwami członkowskimi nie zostałyby osiągnięty za pomocą zdecentralizowanych rozwiązań krajowych, a uzyskanie takich wyników byłoby niemożliwe na szczeblu państw członkowskich. 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 państwami członkowskimi UE. Ponadto Europol i nowa Europejska Agencja Straży Granicznej i Przybrzeżnej, 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*

1. Faza opracowywania powinna rozpocząć się dopiero po określeniu wszystkich potrzeb związanych z działalnością i wymagań użytkowników końcowych. 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) stałe 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, które wnosi się przedmiotowym rozporządzeniem, poddano kompleksowym dyskusjom przy zapewnieniu pełnej przejrzystości omawianych kwestii na specjalnie poświęconych temu spotkaniach i warsztatach. 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 dwóch badań, których ustalenia uwzględniono przy opracowywaniu niniejszego wniosku:

- oceny technicznej SIS – 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 – 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.

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 bezpieczeństwa⁸⁴. 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.

Co więcej, niniejszy wniosek jest ściśle powiązany z innymi obszarami polityki Unii i uzupełnia tego rodzaju obszary. Obszary te to:

a) bezpieczeństwo wewnętrzne, jak podkreślono w Europejskiej agencji bezpieczeństwa⁸⁵, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, wykrywania ich, prowadzenia dochodzeń w ich sprawach i ścigania ich poprzez umożliwienie organom ścigania przetwarzania danych osobowych osób podejrzanych o udział w aktach terrorystycznych lub w poważnych przestępstwach;

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) Europejskiej Straży Granicznej i Przybrzeżnej⁸⁶ w zakresie, w jakim po pierwsze pracownicy Agencji mają możliwość przeprowadzania analiz ryzyka, a po drugie w zakresie ich dostępu do SIS do celów proponowanego ETIAS. Celem wniosku jest również dostarczenie interfejsu technicznego zapewniającego dostęp do SIS zespołom Europejskiej Straży Granicznej i Przybrzeżnej, zespołom składającym się z personelu realizującego zadania w dziedzinie powrotów oraz członkom zespołu wspierającego 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;

b) 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;

c) ram z Prüm⁸⁷ w zakresie, w jakim zmiany wprowadzone niniejszym wnioskiem w celu umożliwienia identyfikacji osób fizycznych na podstawie odcisków palców (jak i wizerunków twarzy i profili DNA) uzupełniają obowiązujące postanowienia z Prüm dotyczące wzajemnego transgranicznego dostępu on-line do wyznaczonych krajowych baz danych DNA i systemów automatycznej identyfikacji daktyloskopijnej.

⁸⁴ COM(2016) 205 final.

⁸⁵ COM(2015) 185 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 Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.U. L 210 z 6.8.2008, s. 1), oraz decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. w sprawie wdrożenia decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.U. L 210 z 6.8.2008, s. 12).

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

a) zarządzania granicami zewnętrznymi. Niniejszy wniosek uzupełnia przewidzianą nową zasadę kodeksu granicznego Schengen dotyczącą systematycznych kontroli wszystkich podróżnych, w tym obywateli Unii, w odpowiednich bazach danych w momencie wjazdu do strefy Schengen i jej opuszczania, które to kontrole wprowadzono w odpowiedzi na zjawisko zagranicznych bojowników terrorystycznych;

b) systemu wjazdu/wyjazdu⁸⁸ w zakresie, w jakim wniosek ma uwzględniać proponowane wykorzystanie połączenia odcisków palców i wizerunku twarzy jako identyfikatorów biometrycznych na potrzeby funkcjonowania systemu wjazdu/wyjazdu.

c) ETIAS w zakresie, w jakim we wniosku uwzględnia się proponowany system ETIAS, w ramach którego przewiduje się dokładną ocenę bezpieczeństwa, w tym kontrolę w SIS, przeprowadzaną w przypadku obywateli państw trzecich, którzy zamierzają podróżować na terytorium Unii Europejskiej.

⁸⁸

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 (COM(2016) 194 final).

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**

– Okres przygotowawczy w 2017 r.

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

– po którym następuje faza operacyjna.

1.7. Przewidywane tryby zarządzania⁸⁹

☒ **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.

– *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

⁸⁹

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

rozporządzenia w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych) 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. 71 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.

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.

2.2. 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, eu-LISA 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 eu-LISA.

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 WPLYW 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 ⁹⁰ .	państw EFTA ⁹¹	krajów kandydujących ⁹²	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

⁹⁰ Środki zróżnicowane / środki niezróżnicowane.

⁹¹ EFTA: Europejskie Stowarzyszenie Wolnego Handlu.

⁹² 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 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 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 płatności	=2+2a +3	6,234	20,259	20,259	46,752

Dział wieloletnich ramfinansowych	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 płatności	=2+2a +3	2,710	8,103	4,861	15,674

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 ramfinansowych		5	„Wydatki administracyjne”						
			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							

w mln EUR (do trzech miejsc po przecinku)

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 ⁹³	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							

⁹³ 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 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 ⁹⁴	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem	
CEL SZCZEGÓŁOWY nr 1 ⁹⁵ Rozwój systemu krajowego			1		1	1,221	1	1,221										2,442	
CEL SZCZEGÓŁOWY nr 2 Infrastruktura			1		1	17,184	1	17,184										34,368	
KOSZT OGÓŁEM						18,405		18,405										36,810	

⁹⁴ Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).
⁹⁵ Zgodnie z opisem w pkt 1.4.2. „Cel(-e) szczegółowy(-e)…”.

3.2.3.2. 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:

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

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 ⁹⁶	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY nr 1 ⁹⁷ 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 2Konserwacja 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

⁹⁶ Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).
⁹⁷ 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 3Spotkania/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

3.2.3.3. Szacunkowy wpływ na zasoby ludzkie eu-LISA

Streszczenie

- ☐ 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
--	-------------	-------------	-------------	--------

Urzednicy (grupa zaszeregowania AD)				
Urzednicy (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 trzech 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)⁹⁸							
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 ⁹⁹	- 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

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

⁹⁸ CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JED = młodszy oddelegowany ekspert.

⁹⁹ W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA”).

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:

Urzednicy i pracownicy zatrudnieni na czas okreslony	
Personel zewnetrzny	

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 rozporządzenia 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 związanych z modernizacją SIS II i jego funkcji 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 ¹⁰⁰						
		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.

¹⁰⁰

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.