ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2018/1861

z dnia 28 listopada 2018 r.

w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([1]),

a także mając na uwadze, co następuje:

(1) System Informacyjny Schengen (SIS) stanowi zasadnicze narzędzie stosowania postanowień dorobku Schengen, który został włączony w ramy Unii Europejskiej. SIS jest jednym z głównych środków kompensacyjnych, które przyczyniają się do utrzymania wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii poprzez wspomaganie współpracy operacyjnej między właściwymi organami krajowymi, w szczególności strażą graniczną, policją, organami celnymi, organami imigracyjnymi oraz organami odpowiadającymi za zapobieganie przestępstwom, ich wykrywanie, prowadzenie w ich sprawie postępowań przygotowawczych lub ich ściganie lub za wykonywanie kar.

(2) SIS został pierwotnie ustanowiony na mocy postanowień tytułu IV Konwencji wykonawczej z dnia 19 czerwca 1990 r. do układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach ([2]) („konwencja wykonawcza do układu z Schengen"). Opracowanie systemu SIS drugiej generacji (SIS II) powierzono Komisji na mocy rozporządzenia Rady (WE) nr 2424/2001 ([3]) i decyzji Rady 2001/886/WSiSW ([4]). Został on następnie ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 1987/2006 ([5]) i decyzją Rady 2007/533/WSiSW ([6]). SIS II zastąpił SIS utworzony na mocy konwencji wykonawczej do układu z Schengen.

(3) Trzy lata po uruchomieniu SIS II Komisja przeprowadziła ocenę systemu zgodnie z rozporządzeniem (WE) nr 1987/2006 oraz decyzją 2007/533/WSiSW. W dniu 21 grudnia 2016 r. Komisja przekazała Parlamentowi Europejskiemu i Radzie sprawozdanie 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. Zalecenia zawarte w tych dokumentach powinny znaleźć odzwierciedlenie, w stosownych przypadkach, w niniejszym rozporządzeniu.

(4) Niniejsze rozporządzenie stanowi podstawę prawną systemu SIS w kwestiach objętych zakresem stosowania rozdziału 2 tytułu V części trzeciej Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 ([7]) stanowi podstawę prawną systemu SIS w kwestiach objętych zakresem stosowania rozdziałów 4 i 5 tytułu V części trzeciej TFUE.

([1]) Stanowisko Parlamentu Europejskiego z dnia 24 października 2018 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 19 listopada 2018 r.

([2]) Dz.U. L 239 z 22.9.2000, s. 19.

([3]) Rozporządzenie Rady (WE) nr 2424/2001 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. 4).

([4]) 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).

([5]) Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 381 z 28.12.2006, s. 4).

([6]) 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).

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmieniające i uchylające decyzję Rady 2007/533/WSiSW oraz uchylające rozporządzenie (WE) nr 1986/2006 Parlamentu Europejskiego i Rady i decyzję Komisji 2010/261/UE (zob. s. 56 niniejszego Dziennika Urzędowego).

(5) Fakt, że podstawa prawna systemu SIS składa się z odrębnych aktów, nie narusza zasady, że SIS stanowi – i powinien funkcjonować jako – jednolity system informacyjny. Jego elementem powinna być jednolita sieć biur krajowych zwanych biurami SIRENE, które zapewnią wymianę informacji uzupełniających. Niektóre przepisy tych aktów powinny być zatem identyczne.

(6) Należy dokładnie określić przeznaczenie SIS, niektóre elementy jego architektury technicznej i jego finansowanie, ustanowić zasady jego funkcjonowania i użytkowania w całym cyklu oraz określić zakresy odpowiedzialności. Ponadto należy ustalić kategorie danych, które będą wprowadzane do systemu, cele, do jakich dane te mają być wprowadzane i przetwarzane oraz kryteria ich wprowadzania. Konieczne są również zasady dotyczące usuwania wpisów, organów uprawnionych do dostępu do danych, korzystania z danych biometrycznych oraz dalsze zasady w zakresie ochrony i przetwarzania danych.

(7) Wpisy w SIS zawierają wyłącznie informacje niezbędne do zidentyfikowania osób i do podjęcia działań. Państwa członkowskie powinny zatem w razie potrzeby przeprowadzać wymianę informacji uzupełniających związanych z wpisami.

(8) SIS obejmuje system centralny (system centralny SIS) oraz systemy krajowe. Systemy krajowe mogą zawierać pełną lub częściową kopię bazy danych SIS, z której mogą wspólnie korzystać dwa państwa członkowskie lub większa ich liczba. Z uwagi na to, że SIS jest najważniejszym narzędziem wymiany informacji w Europie na potrzeby zapewnienia bezpieczeństwa i skutecznego zarządzania granicami, konieczne jest zapewnienie jego nieprzerwanego funkcjonowania na szczeblu centralnym i krajowym. Dostępność SIS należy ściśle monitorować na szczeblu centralnym i szczeblu państw członkowskich, a wszelkie przypadki jego niedostępności dla użytkowników końcowych należy rejestrować i zgłaszać zainteresowanym stronom na szczeblu krajowym i unijnym. Każde państwo członkowskie powinno utworzyć wersję zapasową swojego systemu krajowego. Państwa członkowskie powinny także zapewnić nieprzerwaną łączność z systemem centralnym SIS dzięki zdublowanym, fizycznie i geograficznie oddzielonym punktom dostępowym. System centralny SIS i infrastruktura łączności powinny funkcjonować w taki sposób, by zapewnić możliwość ich użytkowania przez 24 godziny na dobę, 7 dni w tygodniu. Z tego względu Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (zwana dalej „eu-LISA"), ustanowiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1726 ([1]) powinna wdrożyć – z uwzględnieniem niezależnej oceny skutków oraz analizy kosztów i korzyści – rozwiązania techniczne, które zwiększą niezakłóconą dostępność SIS.

(9) Należy utrzymać podręcznik określający szczegółowe zasady wymiany informacji uzupełniających dotyczących działania, które należy podjąć w następstwie wpisów (zwany dalej „podręcznikiem SIRENE"). Biura SIRENE w każdym państwie członkowskim powinny zapewnić szybką i skuteczną wymianę takich informacji.

(10) Aby zapewnić skuteczną wymianę informacji uzupełniających, w tym informacji na temat podjęcia działania określonego we wpisach, należy wzmocnić funkcjonowanie biur SIRENE poprzez określenie wymogów dotyczących dostępnych zasobów oraz szkoleń użytkowników i czasu na udzielenie odpowiedzi na pytania nadesłane z innych biur SIRENE.

(11) Państwa członkowskie powinny zapewnić, by pracownicy ich biura SIRENE posiadali umiejętności językowe i wiedzę na temat odpowiednich przepisów i zasad proceduralnych niezbędne do wykonywania ich zadań.

(12) W celu umożliwienia pełnego korzystania z funkcji SIS państwa członkowskie powinny zapewnić, by użytkownicy końcowi i pracownicy biur SIRENE przechodzili regularne szkolenia, w tym w zakresie bezpieczeństwa, ochrony danych i jakości danych. Biura SIRENE powinny być włączane w opracowywanie programów szkoleniowych. W miarę możliwości biura SIRENE powinny również przewidzieć organizowanie przynajmniej raz w roku wymiany pracowników z innymi biurami SIRENE. Zachęca się państwa członkowskie do podejmowania odpowiednich działań, które pozwolą uniknąć utraty umiejętności i doświadczenia wynikającej z rotacji pracowników.

(13) Za zarządzanie operacyjne centralnymi komponentami SIS odpowiada eu-LISA. Aby umożliwić eu-LISA przeznaczenie niezbędnych zasobów finansowych i kadrowych pokrywających wszystkie aspekty zarządzania operacyjnego systemem centralnym SIS i infrastrukturą łączności, w niniejszym rozporządzeniu należy szczegółowo określić jej zadania, w szczególności w odniesieniu do technicznych aspektów prowadzenia wymiany informacji uzupełniających.

(14) Bez uszczerbku dla spoczywającego na państwach członkowskich obowiązku zapewnienia, by dane wprowadzane do SIS były prawidłowe, oraz dla roli biur SIRENE jako koordynatorów jakości, eu-LISA powinna być odpowiedzialna za podnoszenie jakości danych poprzez wprowadzenie centralnego narzędzia monitorowania jakości danych oraz powinna przekazywać Komisji i państwom członkowskim sprawozdania w regularnych odstępach czasu. Komisja powinna informować Parlament Europejski i Radę o napotkanych problemach

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1726 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), zmiany rozporządzenia (WE) nr 1987/2006 i decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia (UE) nr 1077/2011 (Dz.U. L 295 z 21.11.2018, s. 99).

związanych z jakością danych. Aby w większym stopniu poprawić jakość danych w SIS, eu-LISA powinna także oferować krajowym podmiotom prowadzącym szkolenia oraz, w miarę możliwości, biurom SIRENE i użytkownikom końcowym szkolenia na temat użytkowania SIS.

(15) Aby umożliwić lepsze monitorowanie użytkowania SIS oraz analizowanie tendencji związanych z presją migracyjną i zarządzaniem granicami, eu-LISA powinna mieć możliwość rozwijania nowoczesnych zdolności w zakresie prowadzenia sprawozdawczości statystycznej z przeznaczeniem dla państw członkowskich, Parlamentu Europejskiego, Rady, Komisji, Europolu i Europejskiej Agencji Straży Granicznej i Przybrzeżnej, bez naruszania integralności danych. Należy zatem utworzyć centralne repozytorium. Statystyki przechowywane w tym repozytorium lub uzyskiwane z niego nie powinny zawierać danych osobowych. Państwa członkowskie powinny przekazywać statystyki dotyczące korzystania z prawa do dostępu, sprostowania nieprawidłowych danych i usuwania danych przechowywanych niezgodnie z prawem w ramach współpracy między organami nadzorczymi a Europejskim Inspektorem Ochrony Danych na podstawie niniejszego rozporządzenia.

(16) Do SIS należy wprowadzić nowe kategorie danych, aby umożliwić użytkownikom końcowym bezzwłoczne podejmowanie uzasadnionych decyzji na podstawie wpisu. W związku z tym wpisy do celu odmowy wjazdu i pobytu powinny zawierać informacje dotyczące decyzji będącej podstawą wpisu. Ponadto w celu ułatwienia identyfikacji i wykrywania przypadków posługiwania się wieloma tożsamościami wpis powinien, w przypadku, gdy takie informacje są dostępne, zawierać odniesienie do dokumentu identyfikacyjnego danej osoby lub jego numer i kopię takiego dokumentu, w miarę możliwości w kolorze.

(17) Właściwe organy powinny mieć możliwość, jeżeli jest to ściśle niezbędne, wprowadzania do SIS konkretnych informacji odnoszących się do wszelkich szczególnych obiektywnych cech fizycznych danej osoby niepodlegających zmianie, takich jak tatuaże, znamiona lub blizny.

(18) Aby zminimalizować ryzyko fałszywych trafień i ograniczyć niepotrzebne działania operacyjne, przy tworzeniu wpisu należy wprowadzić wszelkie stosowne dane, o ile są one dostępne, w szczególności imię danej osoby.

(19) W SIS nie należy przechowywać żadnych danych wykorzystywanych do wyszukiwań, z wyjątkiem rejestrów służących do sprawdzenia, czy dane wyszukiwanie jest zgodne z prawem, do monitorowania zgodności przetwarzania danych z prawem, do monitorowania własnej działalności oraz do zapewniania należytego działania systemów krajowych, a także integralności i bezpieczeństwa danych.

(20) SIS powinien umożliwiać przetwarzanie danych biometrycznych, aby ułatwić niezawodną identyfikację odnośnych osób. Wprowadzanie fotografii, wizerunków twarzy lub danych daktyloskopijnych do SIS oraz wykorzystywanie takich danych powinno być ograniczone do tego, co jest niezbędne do osiągnięcia wyznaczonych celów, powinno być dopuszczalne na mocy prawa Unii, powinno być prowadzone z poszanowaniem praw podstawowych, w tym najlepszego interesu dziecka, oraz powinno być zgodne z prawem Unii dotyczącym ochrony danych, w tym z odpowiednimi przepisami niniejszego rozporządzenia dotyczącymi ochrony danych. Równocześnie w celu zapobieżenia niedogodnościom, jakie może spowodować błędna identyfikacja tych osób, SIS powinien też pozwalać na przetwarzanie danych dotyczących osób, których tożsamość została przywłaszczona, pod warunkiem zastosowania odpowiednich zabezpieczeń i uzyskania w odniesieniu do każdej kategorii danych, w szczególności odbitek linii papilarnych dłoni, zgody danej osoby i przy ścisłym ograniczeniu celów, do których takie dane osobowe mogą być zgodnie z prawem przetwarzane.

(21) Państwa członkowskie powinny wprowadzić niezbędne rozwiązania techniczne, tak aby za każdym razem, gdy użytkownicy końcowi będą uprawnieni do przeprowadzenia wyszukiwania w krajowej bazie danych policji lub bazie imigracyjnej, mogli oni równolegle przeprowadzić wyszukiwanie w SIS z zastrzeżeniem zasad określonych w art. 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 ([1]) i art. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([2]). Dzięki temu SIS będzie mógł działać jako główny środek kompensacyjny na obszarze bez kontroli na granicach wewnętrznych i lepiej uwzględniać transgraniczny wymiar przestępczości i mobilność przestępców.

(22) W niniejszym rozporządzeniu należy określić warunki korzystania z danych daktyloskopijnych, fotografii i wizerunków twarzy w celach identyfikacyjnych i weryfikacyjnych. Wizerunki twarzy i fotografie do celów identyfikacyjnych powinny początkowo być wykorzystywane wyłączne na stałych przejściach granicznych. Takie wykorzystywanie powinno być przedmiotem sprawozdania Komisji potwierdzającego dostępność, niezawodność i gotowość rozwiązań technologicznych.

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

([2]) 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).

(23) Należy zezwolić na przeszukiwanie danych daktyloskopijnych przechowywanych w SIS przy zastosowaniu kompletnych lub niekompletnych zestawów odbitek linii papilarnych palców lub odbitek linii papilarnych dłoni, które znaleziono na miejscu przestępstwa, jeżeli z dużym prawdopodobieństwem można stwierdzić, że należą one do sprawcy poważnego przestępstwa lub przestępstwa terrorystycznego, pod warunkiem że wyszukiwanie przeprowadzane jest równolegle w odpowiednich krajowych bazach danych zawierających dane daktyloskopijne. Szczególną uwagę należy poświęcić ustaleniu norm jakości mających zastosowanie do przechowywania danych biometrycznych.

(24) W przypadku gdy tożsamości danej osoby nie można ustalić w żaden inny sposób, do próby identyfikacji należy wykorzystać dane daktyloskopijne. Identyfikacja danej osoby przy wykorzystaniu danych daktyloskopijnych powinna być dopuszczalna we wszystkich przypadkach.

(25) Państwa członkowskie powinny mieć możliwość tworzenia w SIS odsyłaczy pomiędzy różnymi wpisami. Utworzenie odsyłaczy pomiędzy dwoma wpisami lub większą liczbą wpisów nie powinno mieć wpływu na działanie, które należy podjąć, na termin weryfikacji tych wpisów, ani na prawa do dostępu do nich.

(26) Większy stopień skuteczności, harmonizacji i spójności można osiągnąć poprzez ustanowienie obowiązku wprowadzania do SIS wszystkich zakazów wjazdu wydanych przez właściwe organy krajowe zgodnie z procedurami spełniającymi wymogi dyrektywy Parlamentu Europejskiego i Rady 2008/115/WE ([1]) oraz ustanowienie wspólnych zasad dotyczących wprowadzania wpisów dotyczących odmowy wjazdu i pobytu po powrocie nielegalnie przebywającego obywatela państwa trzeciego. Państwa członkowskie powinny podjąć wszelkie niezbędne działania w celu zapewnienia, by nie wystąpiła luka czasowa między momentem, w którym dany obywatel państwa trzeciego opuścił strefę Schengen, a aktywowaniem wpisu w SIS. Powinno to pozwolić na egzekwowanie zakazów wjazdu na przejściach granicznych na granicach zewnętrznych, i w związku z tym faktycznie uniemożliwić ponowny wjazd do strefy Schengen.

(27) Osoby, w odniesieniu do których podjęto decyzję o odmowie wjazdu i pobytu, powinny mieć prawo do wniesienia odwołania od tych decyzji. Prawo do wniesienia odwołania powinno być zgodne z dyrektywą 2008/115/WE, jeżeli dana decyzja dotyczy powrotu.

(28) Niniejsze rozporządzenie powinno ustanawiać obowiązkowe zasady konsultowania się z organami krajowymi i ich powiadamiania w przypadku, gdy obywatel państwa trzeciego posiada ważny dokument pobytowy lub ważną wizę długoterminową przyznane w jednym państwie członkowskim lub może je tam uzyskać, a inne państwo członkowskie zamierza dokonać lub już dokonało wpisu dotyczącego odmowy wjazdu i pobytu odnoszącego się do danego obywatela państwa trzeciego. W takich sytuacjach straż graniczna, policja i organy imigracyjne mogą mieć poważne wątpliwości. Należy zatem ustanowić obowiązkowe ramy czasowe dotyczące szybkich konsultacji, które powinny dać jednoznaczne wyniki, w celu zapewnienia, by obywatele państw trzecich, którzy są uprawnieni do legalnego pobytu na terytorium państw członkowskich, byli uprawnieni do wjazdu na to terytorium i mogli to zrobić bez trudności, oraz by tym, którzy nie są uprawnieni do wjazdu, ten wjazd uniemożliwić.

(29) W przypadku usunięcia wpisu w SIS w następstwie konsultacji między państwami członkowskimi państwo członkowskie dokonujące wpisu powinno mieć możliwość utrzymania danego obywatela państwa trzeciego w swoim krajowym wykazie wpisów.

(30) Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2004/38/WE Parlamentu Europejskiego i Rady ([2]).

(31) Wpisów nie należy utrzymywać w SIS dłużej, niż jest to konieczne do osiągnięcia konkretnych celów, do których zostały wprowadzone. W terminie trzech lat od wprowadzenia wpisu do SIS państwo członkowskie dokonujące wpisu powinno zweryfikować, czy istnieje potrzeba jego dalszego utrzymywania. Jednakże jeżeli decyzja krajowa, która jest podstawą wpisu, przewiduje okres ważności dłuższy niż trzy lata, wpis należy zweryfikować w terminie pięciu lat. Decyzje o utrzymaniu wpisów dotyczących osób powinny być podejmowane na podstawie wszechstronnej indywidualnej oceny. Państwa członkowskie powinny w przed upływem wyznaczonego terminu weryfikacji przeprowadzać weryfikację wpisów dotyczących osób, a ponadto prowadzić statystyki na temat liczby wpisów dotyczących osób, w przypadku których okres przechowywania został przedłużony.

(32) Wprowadzenie wpisu w SIS, a także przedłużenie jego terminu ważności, powinno podlegać wymogowi zachowania proporcjonalności, poprzez zbadanie, czy konkretny przypadek jest wystarczająco adekwatny, odpowiedni i ważny, by uzasadnione było wprowadzenie wpisu do SIS. W przypadku przestępstw terrorystycznych każdy przypadek należy uznać za wystarczająco adekwatny, odpowiedni i ważny dla uzasadnienia wpisu w SIS. Ze względu na bezpieczeństwo publiczne lub narodowe państwa członkowskie powinny wyjątkowo mieć możliwość niewprowadzania wpisu do SIS, jeśli istnieje prawdopodobieństwo, że utrudniłby on prowadzenie urzędowych lub sądowych dochodzeń, postępowań przygotowawczych lub procedur.

([1]) 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).

([2]) Dyrektywa 2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium państw członkowskich, zmieniająca rozporządzenie (EWG) nr 1612/68 i uchylająca dyrektywy 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG i 93/96/EWG (Dz.U. L 158 z 30.4.2004, s. 77).

(33) Kluczowe znaczenie ma integralność danych SIS. Należy zatem przewidzieć odpowiednie zabezpieczenia przy przetwarzaniu danych SIS na szczeblu centralnym i krajowym w celu zapewnienia bezpieczeństwa danych w całym cyklu. Organy uczestniczące w przetwarzaniu danych powinny być objęte wymogami bezpieczeństwa określonymi w niniejszym rozporządzeniu oraz podlegać jednolitej procedurze zgłaszania incydentów. Ich personel powinien zostać odpowiednio przeszkolony oraz zostać poinformowany o przestępstwach i sankcjach w tym zakresie.

(34) Danych przetwarzanych w SIS oraz powiązanych z nimi informacji uzupełniających podlegających wymianie zgodnie z niniejszym rozporządzeniem nie należy przekazywać ani udostępniać państwom trzecim ani organizacjom międzynarodowym.

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

(36) Bez uszczerbku dla bardziej szczegółowych przepisów ustanowionych w niniejszym rozporządzeniu, które regulują przetwarzanie danych osobowych, do przetwarzania danych osobowych przez państwa członkowskie na podstawie niniejszego rozporządzenia zastosowanie powinno mieć rozporządzenie (UE) 2016/679, z wyjątkiem sytuacji, gdy takiego przetwarzania dokonują właściwe organy krajowe do celów zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, prowadzenia w ich sprawie postępowań przygotowawczych, ich wykrywania lub ich ścigania.

(37) Bez uszczerbku dla bardziej szczegółowych przepisów ustanowionych w niniejszym rozporządzeniu, do przetwarzania zgodnie z niniejszym rozporządzeniem danych osobowych przez właściwe organy krajowe do celów zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych lub ich ścigania lub wykonywania kar zastosowanie powinny mieć krajowe przepisy ustawowe, wykonawcze i administracyjne przyjęte na mocy dyrektywy (UE) 2016/680. Dostęp do danych wprowadzonych do SIS i prawo do wyszukiwania takich danych przez właściwe organy krajowe, które odpowiadają za zapobieganie przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywanie, prowadzenie w ich sprawie postępowań przygotowawczych lub ich ściganie lub wykonywanie kar, podlegają wszystkim odpowiednim przepisom niniejszego rozporządzenia oraz przepisom dyrektywy (UE) 2016/680 transponowanym do prawa krajowego, w szczególności monitorowaniu przez krajowe organy nadzorcze, o których mowa w dyrektywie (UE) 2016/680.

(38) Do przetwarzania danych osobowych przez instytucje i organy Unii podczas wykonywania przez nie swoich obowiązków na mocy niniejszego rozporządzenia zastosowanie powinno mieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 ([1]).

(39) Do przetwarzania danych osobowych przez Europol na mocy niniejszego rozporządzenia zastosowanie powinno mieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 ([2]).

(40) Korzystając z SIS, właściwe organy powinny zapewnić poszanowanie godności i integralności osoby, której dane są przetwarzane. Przetwarzanie danych osobowych do celów niniejszego rozporządzenia nie może prowadzić do dyskryminacji w szczególności ze względu na płeć, pochodzenie rasowe lub etniczne, religię lub przekonania, niepełnosprawność, wiek lub orientację seksualną.

(41) W odniesieniu do zachowania poufności, do urzędników lub innych pracowników, którzy są zatrudnieni i pracują przy SIS, powinny mieć zastosowanie odpowiednie przepisy regulaminu pracowniczego urzędników Unii Europejskiej i warunków zatrudnienia innych pracowników Unii, określone w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68 ([3]) (zwanym dalej „regulaminem pracowniczym").

(42) Zarówno państwa członkowskie, jak i eu-LISA powinny utrzymywać plany bezpieczeństwa, które ułatwią realizację wymogów bezpieczeństwa, a także powinny ze sobą współpracować, tak aby rozpatrywać kwestie bezpieczeństwa ze wspólnego punktu widzenia.

(43) Niezależne krajowe organy nadzorcze, o których mowa w rozporządzeniu (UE) 2016/679 oraz dyrektywie (UE) 2016/680, (zwane dalej „organami nadzorczymi"), powinny monitorować zgodność z prawem przetwarzania danych osobowych przez państwa członkowskie na podstawie niniejszego rozporządzenia, w tym wymiany informacji uzupełniających. Organom nadzorczym należy zapewnić wystarczające zasoby umożliwiające wykonywanie tego zadania. Należy ustanowić prawa do dostępu do danych osobowych przechowywanych w SIS, do ich sprostowania i do ich usuwania przysługujące osobom, których dane dotyczą, a także należy ustanowić późniejsze środki ochrony prawnej przed sądami krajowymi oraz wzajemne uznawanie orzeczeń sądowych. Właściwe jest również wymaganie od państw członkowskich przedstawiania statystyk rocznych.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

([2]) 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 24.5.2016, s. 53).

([3]) Dz.U. L 56 z 4.3.1968, s. 1.

(44) Organy nadzorcze powinny zapewnić, aby co najmniej co cztery lata przeprowadzany był audyt operacji przetwarzania danych w ramach systemów krajowych ich państw członkowskich zgodnie z międzynarodowymi standardami audytu. Audyt powinien być prowadzony przez organy nadzorcze lub organy nadzorcze powinny bezpośrednio zlecić przeprowadzenie audytu niezależnemu audytorowi ds. ochrony danych. Niezależny audytor powinien pozostawać pod kontrolą odpowiednich organów nadzorczych i działać na odpowiedzialność tych organów, które w związku z tym powinny same zatrudniać audytora i określić jasno cel, zakres i metodykę audytu oraz wytyczne i nadzór dotyczące audytu i jego wyników końcowych.

(45) Europejski Inspektor Ochrony Danych powinien monitorować działalność instytucji i organów Unii w odniesieniu do przetwarzania danych osobowych na mocy niniejszego rozporządzenia. Europejski Inspektor Ochrony Danych oraz organy nadzorcze powinny współpracować ze sobą w zakresie monitorowania SIS.

(46) Europejskiemu Inspektorowi Ochrony Danych należy przyznać zasoby wystarczające do wykonywania zadań powierzonych mu na mocy niniejszego rozporządzenia, obejmujące pomoc ze strony osób mających specjalistyczną wiedzę w zakresie danych biometrycznych.

(47) Rozporządzenie (UE) 2016/794 stanowi, że Europol ma wspierać i wzmacniać działania prowadzone przez właściwe organy krajowe oraz współpracę między tymi organami w zakresie zwalczania terroryzmu i poważnej przestępczości oraz zapewniać analizę i oceny zagrożeń. Aby ułatwić Europolowi wykonywanie jego zadań, w szczególności w ramach Europejskiego Centrum Zwalczania Przemytu Migrantów, należy przyznać Europolowi dostęp do kategorii wpisów określonych w niniejszym rozporządzeniu.

(48) Aby zniwelować luki w udostępnianiu informacji na temat terroryzmu, w szczególności na temat zagranicznych bojowników terrorystycznych – w przypadku których monitorowanie przemieszczania się ma kluczowe znaczenie – zachęca się państwa członkowskie do udostępniania Europolowi informacji na temat działań związanych z terroryzmem. Udostępnianie informacji powinno następować w drodze wymiany z Europolem informacji uzupełniających dotyczących odpowiednich wpisów. W tym celu Europol powinien ustanowić połączenie z infrastrukturą łączności.

(49) Konieczne jest również określenie w odniesieniu do Europolu jasnych zasad dotyczących przetwarzania i pobierania danych SIS w celu umożliwienia kompleksowego użytkowania SIS, pod warunkiem przestrzegania norm ochrony danych zgodnie z niniejszym rozporządzeniem i rozporządzeniem (UE) 2016/794. Jeżeli w wyniku przeprowadzonych przez siebie wyszukiwań w SIS Europol stwierdzi istnienie wpisu wprowadzonego przez państwo członkowskie, nie będzie mógł podjąć wymaganego działania. Dlatego Europol powinien poinformować o tym dane państwo członkowskie w drodze wymiany informacji uzupełniających z odpowiednim biurem SIRENE, umożliwiając temu państwu członkowskiemu podjęcie dalszych działań w tej sprawie.

(50) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624 ([1]) stanowi – na potrzeby tego rozporządzenia – że przyjmujące państwo członkowskie ma upoważnić członków zespołów, o których mowa w art. 2 pkt 8 tego rozporządzenia, rozmieszczonych przez Europejską Agencję Straży Granicznej i Przybrzeżnej, do korzystania z unijnych baz danych, w przypadku gdy jest to niezbędne do realizacji celów operacyjnych określonych w planie operacyjnym w odniesieniu do odpraw granicznych, ochrony granic i powrotów. Inne właściwe agencje Unii, w szczególności Europejski Urząd Wsparcia w dziedzinie Azylu i Europol, również mogą rozmieszczać – w ramach zespołów wspierających zarządzanie migracjami – ekspertów, którzy nie są pracownikami tych agencji Unii. Celem rozmieszczenia zespołów, o których mowa w art. 2 pkt 8 i 9 tego rozporządzenia, jest zapewnienie wsparcia technicznego i operacyjnego wnioskującym państwom członkowskim, zwłaszcza tym zmagającym się z wyjątkowo trudnymi wyzwaniami migracyjnymi. Aby zespoły, o których mowa w art. 2 pkt 8 i 9 rozporządzenia (UE) 2016/1624, mogły realizować swoje zadania, potrzebują one dostępu do SIS za pośrednictwem interfejsu technicznego Europejskiej Agencji Straży Granicznej i Przybrzeżnej łączącego ją z systemem centralnym SIS. Jeżeli w wyniku przeprowadzonych wyszukiwań w SIS zespoły, o których mowa w art. 2 pkt 8 i 9 tego rozporządzenia, lub zespoły pracowników stwierdzą istnienie wpisu wprowadzonego przez państwo członkowskie, członek zespołu lub pracownik nie będzie mógł podjąć wymaganego działania, chyba że został do tego upoważniony przez przyjmujące państwo członkowskie. Dlatego przyjmujące państwo członkowskie powinno zostać o tym poinformowane, co umożliwi mu podjęcie dalszych działań w tej sprawie. Przyjmujące państwo członkowskie powinno, w drodze wymiany informacji uzupełniających, powiadomić o trafieniu państwo członkowskie dokonujące wpisu.

(51) Niektóre aspekty SIS nie mogą zostać wyczerpująco ujęte w niniejszym rozporządzeniu ze względu na ich techniczny charakter, wysoki poziom szczegółowości i potrzebę regularnej aktualizacji. Dotyczy to na przykład technicznych zasad wprowadzania danych, aktualizacji, usuwania i wyszukiwania danych, jakości danych i zasad dotyczących danych biometrycznych, zasad dotyczących zgodności i hierarchii poszczególnych wpisów, odsyłaczy

([1]) 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).

pomiędzy wpisami oraz prowadzenia wymiany informacji uzupełniających. W związku z tym należy powierzyć Komisji uprawnienia wykonawcze w zakresie tych aspektów. Techniczne zasady dotyczące wyszukiwania wpisów powinny uwzględniać sprawne funkcjonowanie aplikacji krajowych.

(52) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([1]). Procedury przyjmowania aktów wykonawczych na mocy niniejszego rozporządzenia i rozporządzenia (UE) 2018/1862 powinny być takie same.

(53) W celu zapewnienia przejrzystości, po upływie dwóch lat od rozpoczęcia eksploatacji SIS na podstawie niniejszego rozporządzenia, eu-Lisa powinna sporządzić sprawozdanie na temat technicznych aspektów funkcjonowania systemu centralnego SIS i infrastruktury łączności, w tym kwestii ich bezpieczeństwa, oraz na temat dwustronnej i wielostronnej wymiany informacji uzupełniających. Komisja powinna dokonywać ogólnej oceny co cztery lata.

(54) Aby zapewnić sprawne funkcjonowanie SIS, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w odniesieniu do określenia warunków, w jakich – poza stałymi przejściami granicznymi –powinno być dozwolone wykorzystywanie fotografii i wizerunków twarzy do identyfikacji osób. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa ([2]). W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowywaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowywaniem aktów delegowanych.

(55) Ponieważ cele niniejszego rozporządzenia, czyli ustanowienie unijnego systemu informacyjnego i wymiany powiązanych informacji uzupełniających oraz dotyczących ich uregulowań, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na swój charakter możliwe jest ich lepsze ich osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej (TUE). Zgodnie z zasadą proporcjonalności, określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(56) Niniejsze rozporządzenie respektuje prawa podstawowe i jest zgodne z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej. W szczególności niniejsze rozporządzenie zapewnia pełną ochronę danych osobowych zgodnie z art. 8 Karty praw podstawowych Unii Europejskiej, a jednocześnie dążyć do zapewnienia bezpiecznego otoczenia wszystkim osobom przebywającym na terytorium Unii oraz ochrony migrantów o nieuregulowanym statusie przed wykorzystywaniem i byciem przedmiotem handlu ludźmi. W przypadkach odnoszących się do dzieci należy przede wszystkim brać pod uwagę najlepszy interes dziecka.

(57) Szacowane koszty modernizacji systemów krajowych oraz wprowadzenia nowych funkcji przewidzianych w niniejszym rozporządzeniu są niższe niż kwota pozostała w linii budżetowej przeznaczonej na inicjatywę na rzecz inteligentnych granic w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 515/2014 ([3]). W związku z powyższym kwotę przypisaną zgodnie z rozporządzeniem (UE) nr 515/2014 na opracowywanie systemów informatycznych wspierających zarządzanie przepływami migracyjnymi przez granice zewnętrzne należy przydzielić państwom członkowskim i eu-LISA. Należy monitorować finansowe koszty modernizacji SIS oraz wdrożenia niniejszego rozporządzenia. W przypadku wyższych szacowanych kosztów w celu wsparcia państw członkowskich należy udostępnić unijne środki finansowe zgodnie z mającymi zastosowanie wieloletnimi ramami finansowymi.

(58) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do TUE i do TFUE, 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 swojego prawa krajowego.

([1]) 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).

([2]) Dz.U. L 123 z 12.5.2016, s. 1.

([3]) 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 oraz uchylające decyzję nr 574/2007/WE (Dz.U. L 150 z 20.5.2014, s. 143).

(59) Niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, które nie mają zastosowania do Zjednoczonego Królestwa zgodnie z decyzją Rady 2000/365/WE ([1]); Zjednoczone Królestwo nie uczestniczy w związku z tym w przyjęciu niniejszego rozporządzenia i nie jest nim związane ani go nie stosuje.

(60) Niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, które nie mają zastosowania do Irlandii zgodnie z decyzją Rady 2002/192/WE ([2]); Irlandia nie uczestniczy w związku z tym w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje.

(61) W odniesieniu do Islandii i Norwegii niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([3]), które wchodzą w zakres obszaru, o którym mowa w art. 1 lit. G decyzji Rady 1999/437/WE ([4]).

(62) W odniesieniu do Szwajcarii niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([5]), które wchodzą w zakres obszaru, o którym mowa w art. 1 lit. G decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2008/146/WE ([6]).

(63) W odniesieniu do Liechtensteinu niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu o przystąpieniu Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([7]), które wchodzą w zakres obszaru, o którym mowa w art. 1 pkt G decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2011/350/UE ([8]).

(64) W odniesieniu do Bułgarii i Rumunii niniejsze rozporządzenie jest aktem opartym na dorobku Schengen lub w inny sposób z nim związanym w rozumieniu, art. 4 ust. 2 Aktu przystąpienia z 2005 r. i należy je odczytywać w związku z decyzjami Rady 2010/365/UE ([9]) i (UE) 2018/934 ([10]).

(65) W odniesieniu do Chorwacji, niniejsze rozporządzenie jest aktem opartym na dorobku Schengen lub w inny sposób z nim związanym w rozumieniu art. 4 ust. 2 Aktu przystąpienia z 2011 r. i należy je odczytywać w związku z decyzją Rady (UE) 2017/733 ([11]).

(66) W odniesieniu do Cypru niniejsze rozporządzenie jest aktem opartym na dorobku Schengen lub w inny sposób z nim związanym w rozumieniu art. 3 ust. 2 Aktu przystąpienia z 2003 r.

(67) Niniejsze rozporządzenie wprowadza szereg usprawnień w SIS, które poprawią jego skuteczność, zwiększą ochronę danych i poszerzą prawa do dostępu. Niektóre z tych uprawnień nie wiążą się ze złożonymi zmianami technicznymi, inne zaś wymagają zmian technicznych o różnym zakresie. W celu zapewnienia, by usprawnienia zostały udostępnione użytkownikom końcowym jak najszybciej, niniejsze rozporządzenie wprowadza zmiany do rozporządzenia (WE) nr 1987/2006 obejmujące kilka etapów. Część usprawnień systemu powinna mieć

([1]) Decyzja Rady 2000/365/WE z dnia 29 maja 2000 r. dotycząca wniosku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o zastosowaniu wobec niego niektórych przepisów dorobku Schengen (Dz.U. L 131 z 1.6.2000, s. 43).

([2]) Decyzja Rady 2002/192/WE z dnia 28 lutego 2002 r. dotycząca wniosku Irlandii o zastosowanie wobec niej niektórych przepisów dorobku Schengen (Dz.U. L 64 z 7.3.2002, s. 20).

([3]) Dz.U. L 176 z 10.7.1999, s. 36.

([4]) Decyzja Rady 1999/437/WE z dnia 17 maja 1999 r. w sprawie niektórych warunków stosowania Układu zawartego przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącego włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen (Dz.U. L 176 z 10.7.1999, s. 31).

([5]) Dz.U. L 53 z 27.2.2008, s. 52.

([6]) Decyzja Rady 2008/146/WE z dnia 28 stycznia 2008 r. w sprawie zawarcia w imieniu Wspólnoty Europejskiej 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 53 z 27.2.2008, s. 1).

([7]) Dz.U. L 160 z 18.6.2011, s. 21.

([8]) 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).

([9]) Decyzja Rady 2010/365/UE 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).

([10]) Decyzja Rady (UE) 2018/934 z dnia 25 czerwca 2018 r. w sprawie wprowadzenia w życie w Republice Bułgarii i w Rumunii pozostałych przepisów dorobku Schengen dotyczących Systemu Informacyjnego Schengen (Dz.U. L 165 z 2.7.2018, s. 37).

([11]) Decyzja Rady (UE) 2017/733 z dnia 25 kwietnia 2017 r. w sprawie stosowania w Republice Chorwacji przepisów dorobku Schengen dotyczących Systemu Informacyjnego Schengen (Dz.U. L 108 z 26.4.2017, s. 31).

zastosowanie natychmiast po wejściu w życie niniejszego rozporządzenia, natomiast pozostałe usprawnienia należy zacząć stosować jeden rok lub dwa lata po jego wejściu w życie. Niniejsze rozporządzenie należy stosować w całości w terminie trzech lat po jego wejściu w życie. Stopniowe wdrażanie niniejszego rozporządzenia powinno być ściśle monitorowane, tak aby zapobiec opóźnieniom w jego stosowaniu.

(68) Rozporządzenie (WE) nr 1987/2006 należy uchylić ze skutkiem od dnia rozpoczęcia pełnego stosowania niniejszego rozporządzenia.

(69) Zgodnie z art. 28 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 45/2001 ([1]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 3 maja 2017 r.,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Cel ogólny 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 i porządku publicznego oraz zagwarantowanie bezpieczeństwa na terytorium państw członkowskich, a także zapewnienie stosowania postanowień rozdziału 2 tytułu V części trzeciej TFUE w odniesieniu do przepływu osób na terytorium państw członkowskich.

Artykuł 2

Przedmiot

1. Niniejsze rozporządzenie określa warunki i procedury wprowadzania do SIS i przetwarzania wpisów w SIS dotyczących obywateli państw trzecich oraz wymiany informacji uzupełniających i danych dodatkowych na potrzeby odmowy wjazdu i pobytu na terytorium państw członkowskich.

2. Niniejsze rozporządzenie ustanawia również przepisy dotyczące architektury technicznej SIS, obowiązków państw członkowskich i Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (zwanej dalej „eu-LISA"), przetwarzania danych, praw odnośnych osób oraz odpowiedzialności.

Artykuł 3

Definicje

Na użytek niniejszego rozporządzenia stosuje się następujące definicje:

1) „wpis" oznacza zestaw danych wprowadzonych do SIS, które umożliwiają właściwym organom zidentyfikowanie osoby w celu podjęcia konkretnego działania;

2) „informacje uzupełniające" oznaczają informacje, które nie są częścią danych zawartych we wpisach przechowywanych w SIS, ale są związane z wpisami w SIS, i które podlegają wymianie za pośrednictwem biur SIRENE:

   a) w celu umożliwienia państwom członkowskim wzajemnej konsultacji lub wzajemnego informowania się podczas wprowadzania wpisu;

   b) w celu umożliwienia podjęcia odpowiedniego działania po uzyskaniu trafienia;

   c) w przypadku niemożności podjęcia wymaganego działania;

   d) w przypadku rozwiązywania kwestii jakości danych SIS;

   e) w przypadku rozwiązywania kwestii zgodności i priorytetu wpisów;

   f) w przypadku rozwiązywania kwestii związanych z prawami do dostępu;

3) „dane dodatkowe" oznaczają dane przechowywane w SIS – i związane z wpisami w SIS – które mają być natychmiast dostępne dla właściwych organów, gdy osobę, w odniesieniu do której wprowadzono dane do SIS, zlokalizowano w wyniku wyszukiwania przeprowadzonego w SIS;

([1]) 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).

4) „obywatel państwa trzeciego" oznacza osobę niebędącą obywatelem Unii w rozumieniu art. 20 ust. 1 TFUE, z wyjątkiem osób, którym przysługuje – na mocy umów pomiędzy Unią lub Unią i jej państwami członkowskimi, z jednej strony, a państwami trzecimi, z drugiej strony – prawo do swobodnego przemieszczania się równoważne prawu przysługującemu obywatelom Unii;

5) „dane osobowe" oznaczają dane osobowe zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

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

7) „dopasowanie" oznacza łączne wystąpienie następujących elementów:

   a) wyszukiwanie w SIS przeprowadza użytkownik końcowy;

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

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

8) „trafienie" oznacza dopasowanie, które spełnia następujące kryteria:

   a) zostało potwierdzone przez:

      (i) użytkownika końcowego; lub

      (ii) właściwy organ zgodnie z procedurami krajowymi, w przypadku gdy dane dopasowanie opierało się na porównaniu danych biometrycznych;

   oraz

   b) wymagane jest podjęcie dalszych działań;

9) „państwo członkowskie dokonujące wpisu" oznacza państwo członkowskie, które wprowadziło wpis do SIS;

10) „przyznające państwo członkowskie" oznacza państwo członkowskie, które rozważa przyznanie dokumentu pobytowego lub wizy długoterminowej lub przedłużenie ich ważności lub które przyznało dokument pobytowy lub wizę długoterminową lub przedłużyło ich ważność i które jest zaangażowane w procedurę konsultacji z innym państwem członkowskim;

11) „wykonujące państwo członkowskie" oznacza państwo członkowskie, które podejmuje lub podjęło wymagane działania po uzyskaniu trafienia;

12) „użytkownik końcowy" oznacza członka personelu właściwego organu uprawnionego do przeprowadzenia wyszukiwania bezpośrednio w CS-SIS, N.SIS lub ich kopii technicznej;

13) „dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych lub fizjologicznych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby fizycznej, a mianowicie fotografie, wizerunki twarzy i dane daktyloskopijne;

14) „dane daktyloskopijne" oznaczają dane dotyczące odbitek linii papilarnych palców i odbitek linii papilarnych dłoni, które z powodu ich niepowtarzalnego charakteru i układu cech szczególnych umożliwiają przeprowadzenie dokładnych i dających jednoznaczne wyniki porównań odnośnie do tożsamości danej osoby;

15) „wizerunek twarzy" oznacza cyfrowe obrazy twarzy mające dostateczną rozdzielczość i jakość, aby można je było wykorzystywać na potrzeby zautomatyzowanego dopasowywania biometrycznego;

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

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

18) „przestępstwa terrorystyczne" oznaczają przestępstwa w rozumieniu prawa krajowego, o których mowa w art. 3–14 dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 ([1]), lub – w przypadku państw członkowskich niezwiązanych tą dyrektywą – które są równoważne jednemu z przestępstw wymienionych w tej dyrektywie;

19) „dokument pobytowy" oznacza dokument pobytowy zdefiniowany w art. 2 pkt 16 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/399 ([2]);

20) „wiza długoterminowa" oznacza wizę długoterminową, o której mowa w art. 18 ust. 1 konwencji wykonawczej do układu z Schengen;

21) „zagrożenie dla zdrowia publicznego" oznacza zagrożenie dla zdrowia publicznego zdefiniowane w art. 2 pkt 21 rozporządzeniu (UE) 2016/399.

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. L 88 z 31.3.2017, s. 6).

([2]) Rozporządzenie 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) (Dz.U. L 77 z 23.3.2016. s. 1).

Artykuł 4

Architektura techniczna i sposoby funkcjonowania SIS

1. SIS składa się z:

a) systemu centralnego (zwanego dalej „systemem centralnym SIS") składającego się z:

(i) funkcji wsparcia technicznego (CS-SIS), zawierającej bazę danych (zwaną dalej „bazą danych SIS") oraz wersję zapasową CS-SIS;

(ii) jednolitego interfejsu krajowego (NI-SIS);

b) systemu krajowego (N.SIS) w każdym państwie członkowskim, składającego się z krajowych systemów danych, które łączą się z systemem centralnym SIS w tym co najmniej jednej krajowej lub wspólnej wersji zapasowej N.SIS; oraz

c) infrastruktury łączności pomiędzy CS-SIS, wersją zapasową CS-SIS i NI-SIS (zwanej dalej „infrastrukturą łączności"), która zapewnia zaszyfrowaną wirtualną sieć na potrzeby danych SIS oraz wymiany danych między biurami SIRENE, o której mowa w art. 7 ust. 2.

N.SIS, o którym mowa w lit. b), może zawierać plik danych (zwany dalej „kopią krajową"), zawierający pełną lub częściową kopię bazy danych SIS. Dwa państwa członkowskie lub większa ich liczba mogą utworzyć w jednym ze swoich N.SIS wspólną kopię, z której mogą wspólnie korzystać. Taka wspólna kopia uważana jest za kopię krajową każdego z tych państw członkowskich.

Ze wspólnej wersji zapasowej N.SIS, o której mowa w lit. b), mogą wspólnie korzystać dwa państwa członkowskie lub większa ich liczba. W takich przypadkach, wspólną wersję zapasową N.SIS traktuje się ją jako wersję zapasową N.SIS każdego z tych państw członkowskich. Aby zapewnić użytkownikom końcowym niezakłóconą dostępność, istnieje możliwość jednoczesnego korzystania z N.SIS i jego wersji zapasowej.

Państwa członkowskie zamierzające utworzyć wspólną kopię lub wspólną wersję zapasową N.SIS, z których mogą wspólnie korzystać, uzgadniają na piśmie swoje odpowiednie obowiązki. O uzgodnieniach tych informują one Komisję.

Infrastruktura łączności wspiera i pomaga zapewnić niezakłóconą dostępność SIS. Obejmuje ona redundantne i rozdzielne ścieżki dla połączeń między CS-SIS i wersją zapasową CS-SIS, a także redundantne i rozdzielne ścieżki dla połączeń między każdym krajowym punktem dostępu do sieci SIS oraz CS-SIS i wersją zapasową CS-SIS.

2. Państwa członkowskie wprowadzają, aktualizują, usuwają i wyszukują dane SIS korzystając ze swoich N. SIS. Państwa członkowskie korzystające z częściowej lub pełnej krajowej kopii lub częściowej lub pełnej wspólnej kopii udostępniają tę kopię do celów przeprowadzania zautomatyzowanych wyszukiwań na terytorium każdego z tych państw członkowskich. Częściowa krajowa lub wspólna kopia zawiera co najmniej dane wymienione w art. 20 ust. 2 lit. a)–v). Przeszukiwanie plików danych przechowywanych w N.SIS innych państw członkowskich nie jest możliwe, z wyjątkiem sytuacji, gdy dotyczy to wspólnych kopii.

3. CS-SIS wykonuje techniczne funkcje nadzorcze i administracyjne i posiada wersję zapasową CS-SIS, która jest w stanie zapewnić wszystkie funkcje głównego CS-SIS w przypadku jego awarii. CS-SIS i wersja zapasowa CS-SIS znajdują się w dwóch centrach technicznych eu-LISA.

4. eu-LISA wdraża rozwiązania techniczne mające na celu zwiększenie niezakłóconej dostępności SIS poprzez jednoczesne funkcjonowanie CS-SIS i wersji zapasowej CS-SIS, o ile taka wersja zapasowa CS-SIS jest w stanie zagwarantować funkcjonowanie SIS w przypadku awarii, albo poprzez duplikację systemu lub jego komponentów. Niezależnie od wymogów proceduralnych określonych w art. 10 rozporządzenia (UE) 2018/1726, eu-LISA przygotuje, nie później niż dnia 28 grudnia 2019 r., opracowanie dotyczące opcji w zakresie rozwiązań technicznych, zawierające niezależną ocenę skutków oraz analizę kosztów i korzyści.

5. Jeżeli jest to konieczne w wyjątkowych okolicznościach, eu-LISA może przygotować, jako tymczasowe rozwiązanie, dodatkową kopię bazy danych SIS.

6. CS-SIS zapewnia usługi niezbędne do wprowadzania i przetwarzania danych SIS, w tym do prowadzenia wyszukiwań w bazie danych SIS. CS-SIS zapewnia państwom członkowskim korzystającym z krajowej lub wspólnej kopii:

a) aktualizacje kopii krajowych w trybie online;

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

c) czynności związane z inicjalizacją i odtwarzaniem kopii krajowych.

7. CS-SIS zapewnia niezakłóconą dostępność.

Artykuł 5

Koszty

1. Koszty funkcjonowania, utrzymania i dalszego rozwijania systemu centralnego SIS i infrastruktury łączności są pokrywane z budżetu ogólnego Unii. Koszty te obejmują także koszty prac przeprowadzanych w odniesieniu do CS-SIS w celu zapewnienia usług, o których mowa w art. 4 ust. 6.

2. W celu pokrycia kosztów wdrażania niniejszego rozporządzenia przydziela się finansowanie z puli środków w wysokości 791 mln EUR przewidzianej w art. 5 ust. 5 lit. b) rozporządzenia (UE) nr 515/2014.

3. Z puli środków, o której mowa w ust. 2, i bez uszczerbku dla dalszego finansowania w tym celu z innych źródeł budżetu ogólnego Unii, kwotę w wysokości 31 098 000 EUR przydziela się eu-LISA. Finansowanie takie realizowane jest w ramach zarządzania pośredniego i przyczynia się do wprowadzania wymaganych na mocy niniejszego rozporządzenia udoskonaleń technicznych dotyczących systemu centralnego SIS i infrastruktury łączności, a także powiązanych działań szkoleniowych.

4. Z puli środków, o której mowa w ust. 2, państwa członkowskie, które uczestniczą w stosowaniu rozporządzenia (UE) nr 515/2014, oprócz podstawowego przydziału środków otrzymują dodatkowy ogólny przydział w wysokości 36 810 000 EUR rozdzielany w równych częściach w formie płatności ryczałtowej. Finansowanie takie realizowane jest w ramach zarządzania dzielonego i jest w całości przeznaczane na szybką i skuteczną modernizację odnośnych systemów krajowych, zgodnie z wymogami niniejszego rozporządzenia.

5. Koszty utworzenia, funkcjonowania, utrzymania i dalszego rozwijania każdego N.SIS ponosi odnośne państwo członkowskie.

ROZDZIAŁ II

OBOWIĄZKI PAŃSTW CZŁONKOWSKICH

Artykuł 6

Systemy krajowe

Każde państwo członkowskie odpowiada za utworzenie, funkcjonowanie, utrzymanie i dalsze rozwijanie swojego N.SIS oraz za przyłączenie go do NI-SIS.

Każde państwo członkowskie odpowiada za zapewnienie użytkownikom końcowym niezakłóconej dostępności danych SIS.

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

Artykuł 7

Urząd N.SIS i biuro SIRENE

1. Każde państwo członkowskie wyznacza organ (zwany dalej „urzędem N.SIS"), który na szczeblu centralnym odpowiada za N.SIS tego państwa.

Organ ten odpowiada za sprawne funkcjonowanie i bezpieczeństwo N.SIS, zapewnia właściwym organom dostęp do SIS i stosuje niezbędne środki, aby zapewnić przestrzeganie niniejszego rozporządzenia. Odpowiada on za zapewnienie, aby wszystkie funkcje SIS były we właściwy sposób udostępniane użytkownikom końcowym.

2. Każde państwo członkowskie wyznacza organ krajowy, który działa przez 24 godziny na dobę, 7 dni w tygodniu, oraz zapewnia wymianę i dostępność wszelkich informacji uzupełniających (zwany „biurem SIRENE") zgodnie z podręcznikiem SIRENE. Każde biuro SIRENE pełni w swoim państwie członkowskim rolę jedynego punktu kontaktowego właściwego do wymiany informacji uzupełniających dotyczących wpisów oraz do ułatwiania podejmowania wymaganych działań, w przypadku gdy do SIS wprowadzono wpisy dotyczące osób, które następnie zostały zlokalizowane po uzyskaniu trafienia.

Każde biuro SIRENE musi mieć, zgodnie z prawem krajowym, łatwy bezpośredni lub pośredni dostęp do wszelkich stosownych informacji krajowych, w tym krajowych baz danych i wszelkich informacji dotyczących wpisów swojego państwa członkowskiego, a także do fachowego doradztwa, tak by móc podejmować działania w odpowiedzi na wnioski o informacje uzupełniające w szybki sposób i w terminach określonych w art. 8.

Biura SIRENE koordynują weryfikację jakości informacji wprowadzonych do SIS. W tym celu mają dostęp do danych przetwarzanych w SIS.

3. Państwa członkowskie przekazują eu-LISA informacje o swoim urzędzie N.SIS i swoim biurze SIRENE. eu-LISA publikuje wykaz urzędów N.SIS i biur SIRENE wraz z wykazem, o którym mowa w art. 41 ust. 8.

Artykuł 8

Wymiana informacji uzupełniających

1. Wymiana informacji uzupełniających prowadzona jest zgodnie z zasadami zawartymi w podręczniku SIRENE i za pośrednictwem infrastruktury łączności. Państwa członkowskie zapewniają niezbędne zasoby techniczne i ludzkie w celu zapewnienia ciągłej dostępności oraz terminowej i skutecznej wymiany informacji uzupełniających. W przypadku gdy infrastruktura łączności jest niedostępna, państwa członkowskie wykorzystują inne odpowiednio zabezpieczone środki techniczne do prowadzenia wymiany informacji uzupełniających. Wykaz odpowiednio zabezpieczonych środków technicznych ustanawia się w podręczniku SIRENE.

2. Informacje uzupełniające są wykorzystywane wyłącznie w celu, w którym zostały przekazane zgodnie z art. 49, chyba że uzyskana zostanie uprzednia zgoda państwa członkowskiego dokonującego wpisu na inne wykorzystanie.

3. Biura SIRENE realizują swoje zadania w sposób szybki i skuteczny, w szczególności udzielając odpowiedzi na wniosek o informacje uzupełniające w jak najszybszym terminie, lecz nie później niż 12 godzin od jego otrzymania.

Wnioski o informacje uzupełniające mające najwyższy priorytet oznacza się w formularzach SIRENE jako „PILNE", podając przy tym uzasadnienie pilnego charakteru danej sprawy.

4. Komisja przyjmuje akty wykonawcze w celu ustanowienia szczegółowych zasad dotyczących zadań biur SIRENE wynikających z niniejszego rozporządzenia oraz zasad wymiany informacji uzupełniających – w formie podręcznika zatytułowanego „Podręcznik SIRENE". Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

Artykuł 9

Zgodność pod względem technicznym i funkcjonalnym

1. Tworząc swój N.SIS, każde państwo członkowskie przestrzega wspólnych norm, protokołów i procedur technicznych mających na celu zapewnienie kompatybilności jego N.SIS z systemem centralnym SIS na potrzeby szybkiego i skutecznego przesyłania danych.

2. Jeżeli państwo członkowskie korzysta z kopii krajowej, zapewnia ono – wykorzystując usługi zapewniane przez CS-SIS i dzięki zautomatyzowanym aktualizacjom, o których mowa w art. 4 ust. 6 – by dane przechowywane w kopii krajowej były identyczne i spójne z danymi w bazie danych SIS oraz by wyszukiwanie przeprowadzane w jego kopii krajowej prowadziło do wyniku równoważnego wynikowi wyszukiwania w bazie danych SIS.

3. Użytkownicy końcowi otrzymują dane niezbędne do wykonania swoich zadań, w szczególności i w razie potrzeby, wszelkie dostępne dane umożliwiające identyfikację osoby, której dane dotyczą, oraz podjęcie wymaganego działania.

4. Państwa członkowskie i eu-LISA przeprowadzają regularne testy w celu zweryfikowania technicznej zgodności kopii krajowych, o której mowa w ust. 2. Wyniki tych testów są uwzględniane jako część mechanizmu ustanowionego na mocy rozporządzenia Rady (UE) nr 1053/2013 ([1]).

5. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania wspólnych norm, protokołów i procedur technicznych, o których mowa w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

Artykuł 10

Bezpieczeństwo – państwa członkowskie

1. W odniesieniu do swojego N.SIS każde państwo członkowskie przyjmuje niezbędne środki, obejmujące 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) uniemożliwić osobom nieuprawnionym dostęp do infrastruktury przetwarzania danych, wykorzystywanej do przetwarzania danych osobowych (kontrola dostępu do infrastruktury);

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

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

d) zapobiegać nieuprawnionemu wprowadzaniu danych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);

e) zapobiegać korzystaniu z systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników);

f) zapobiegać nieuprawnionemu przetwarzaniu danych w SIS oraz nieuprawnionemu zmienianiu lub usuwaniu danych przetwarzanych w SIS (kontrola wprowadzania danych);

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

h) 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 organom nadzorczym, o których mowa w art. 55 ust. 1, na ich wniosek (profile personelu);

i) zapewnić możliwość weryfikacji i stwierdzania, którym podmiotom można przesyłać dane osobowe za pośrednictwem sprzętu do przesyłu danych (kontrola przesyłu danych);

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

k) zapobiegać nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas transportu nośników danych, w szczególności poprzez zastosowanie odpowiednich technik szyfrowania (kontrola transportu);

l) monitorować skuteczność środków bezpieczeństwa, o których mowa w niniejszym ustępie, oraz stosować konieczne środki organizacyjne dotyczące monitorowania wewnętrznego, aby zapewnić przestrzeganie niniejszego rozporządzenia (kontrolowanie własnej działalności);

m) zapewnić w razie przerwy w działaniu możliwość przywrócenia normalnego funkcjonowania zainstalowanych systemów (odzyskiwanie); oraz

n) zapewnić, by SIS wykonywał właściwie swoje funkcje, by błędy były zgłaszane (niezawodność) i by dane osobowe przechowywane w SIS nie mogły ulec uszkodzeniu w wyniku nieprawidłowego funkcjonowania systemu (integralność).

2. Państwa członkowskie stosują środki równoważne środkom, o których mowa w ust. 1, w odniesieniu do bezpieczeństwa przetwarzania i wymiany informacji uzupełniających, w tym zabezpieczenia pomieszczeń biur SIRENE.

3. Państwa członkowskie stosują środki równoważne środkom, o których mowa w ust. 1 niniejszego artykułu, w odniesieniu do bezpieczeństwa przetwarzania danych SIS przez organy, o których mowa w art. 34.

4. Środki opisane w ust. 1, 2 i 3 mogą stanowić część ogólnego podejścia i planu w zakresie bezpieczeństwa na szczeblu krajowym obejmującego różne systemy informatyczne. W takich przypadkach, wymogi przewidziane w niniejszym artykule i ich stosowanie do SIS muszą zostać wyraźnie wskazane w tym planie, który musi zapewniać ich spełnianie.

Artykuł 11

Poufność – państwa członkowskie

1. Każde państwo członkowskie stosuje, zgodnie ze swoim prawem krajowym, swoje przepisy dotyczące tajemnicy zawodowej lub innych równoważnych obowiązków w zakresie poufności do wszystkich osób i podmiotów, od których wymaga się pracy z danymi SIS i informacjami uzupełniającymi. Wymóg ten ma zastosowanie również po zakończeniu pełnienia urzędu przez te osoby lub po ustaniu ich zatrudnienia, lub po zakończeniu działalności tych podmiotów.

2. W przypadku gdy dane państwo członkowskie współpracuje z wykonawcami zewnętrznymi przy zadaniach związanych z SIS, ściśle monitoruje ono działania wykonawcy, by zapewnić przestrzeganie wszystkich przepisów niniejszego rozporządzenia, w szczególności dotyczących bezpieczeństwa, poufności i ochrony danych.

3. Zarządzania operacyjnego N.SIS lub kopiami technicznymi nie powierza się przedsiębiorstwom prywatnym ani organizacjom prywatnym.

Artykuł 12

Prowadzenie rejestrów na szczeblu krajowym

1. Państwa członkowskie zapewniają rejestrowanie w swoich N.SIS każdego dostępu do danych osobowych w CS-SIS oraz wszelkiej wymiany takich danych w ramach CS-SIS – w celu sprawdzania, czy dane wyszukiwanie jest zgodne z prawem, monitorowania zgodności przetwarzania danych z prawem, monitorowania własnej działalności, zapewnienia należytego działania N.SIS oraz integralności i bezpieczeństwa danych. Wymóg ten nie ma zastosowania do zautomatyzowanych procesów, o których mowa w art. 4 ust. 6 lit. a), b) i c).

2. Zapisy w rejestrze wskazują w szczególności historię wpisu, datę i godzinę przetwarzania danych, dane wykorzystane do wyszukiwania, odniesienie do przetwarzanych danych oraz indywidualne i niepowtarzalne identyfikatory użytkownika dotyczące właściwego organu i osoby przetwarzającej dane.

3. Na zasadzie odstępstwa od ust. 2 niniejszego artykułu, jeżeli wyszukiwanie przeprowadza się z wykorzystaniem danych daktyloskopijnych lub wizerunku twarzy zgodnie z art. 33, zapisy w rejestrze zamiast danych rzeczywistych wskazują rodzaj danych wykorzystanych do wyszukiwania.

4. Zapisy w rejestrze są wykorzystywane wyłącznie do celu, o którym mowa w ust. 1, i są usuwane po upływie trzech lat od ich utworzenia. Zapisy w rejestrze obejmujące historię wpisów są usuwane po upływie trzech lat od usunięcia wpisów.

5. Zapisy w rejestrze mogą być przechowywane dłużej niż przez okresy, o których mowa w ust. 4, jeśli są niezbędne do dalszego prowadzenia procedur monitorowania, które już się rozpoczęły.

6. Właściwe organy krajowe odpowiedzialne za sprawdzanie, czy dane wyszukiwanie jest zgodne z prawem, za monitorowanie zgodności przetwarzania danych z prawem i monitorowanie własnej działalności oraz za zapewnianie należytego działania N.SIS oraz integralności i bezpieczeństwa danych muszą mieć, w granicach swoich uprawnień i na swój wniosek, dostęp do rejestrów do celów wykonywania swoich obowiązków.

Artykuł 13

Monitorowanie własnej działalności

Państwa członkowskie zapewniają, aby każdy organ uprawniony do dostępu do danych SIS podejmował niezbędne środki w celu zapewniania przestrzegania niniejszego rozporządzenia oraz w razie potrzeby współpracował z organem nadzorczym.

Artykuł 14

Szkolenie personelu

1. 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 szkolenie w zakresie bezpieczeństwa danych, praw podstawowych, w tym zasad dotyczących ochrony danych, oraz procedur regulujących przetwarzanie danych określonych w podręczniku SIRENE. Członkowie personelu zostają poinformowani o wszelkich stosownych przepisach dotyczących przestępstw i sankcji, w tym sankcji przewidzianych w art. 59.

2. Państwa członkowskie przyjmują krajowe programy szkoleń w zakresie SIS, które obejmują szkolenia skierowane do użytkowników końcowych oraz do personelu biur SIRENE.

Taki program szkoleń może stanowić część ogólnego programu szkoleniowego na szczeblu krajowym, obejmującego szkolenia w innych odpowiednich dziedzinach.

3. W celu zacieśnienia współpracy między biurami SIRENE co najmniej raz w roku organizuje się na szczeblu Unii wspólne kursy szkoleniowe.

ROZDZIAŁ III

OBOWIĄZKI eu-LISA

Artykuł 15

Zarządzanie operacyjne

1. eu-LISA odpowiada za zarządzanie operacyjne systemem centralnym SIS. eu-LISA – we współpracy z państwami członkowskimi – zapewnia, by w systemie centralnym SIS stosowane były zawsze najlepsze dostępne rozwiązania technologiczne w oparciu o analizę kosztów i korzyści.

2. eu-LISA odpowiada również za następujące zadania związane z infrastrukturą łączności:

a) nadzór;

b) bezpieczeństwo;

c) koordynowanie stosunków między państwami członkowskimi a dostawcą;

d) zadania związane z wykonywaniem budżetu;

e) zakupy i odnawianie; oraz

f) kwestie dotyczące umów.

3. eu-LISA odpowiada również za następujące zadania związane z biurami SIRENE i łącznością między biurami SIRENE:

a) koordynowanie działań w zakresie testowania, zarządzanie tymi działaniami i ich wspieranie;

b) utrzymanie i aktualizowanie specyfikacji technicznych dotyczących wymiany informacji uzupełniających między biurami SIRENE a infrastrukturą łączności; oraz

c) zarządzanie wpływem zmian technicznych, gdy dotyczy on zarówno SIS, jak i wymiany informacji uzupełniających między biurami SIRENE.

4. eu-LISA opracowuje i utrzymuje mechanizm i procedury na potrzeby przeprowadzania kontroli jakości danych w CS-SIS. Przekazuje ona w tym zakresie regularne sprawozdania państwom członkowskim.

eu-LISA przekazuje Komisji regularne sprawozdania, w których uwzględnia napotkane problemy i państwa członkowskie, których problemy te dotyczą.

Komisja przekazuje Parlamentowi Europejskiemu i Radzie regularne sprawozdania na temat napotkanych problemów związanych z jakością danych.

5. eu-LISA wykonuje także zadania związane z organizacją szkoleń na temat technicznego użytkowania SIS oraz środków służących poprawie jakości danych SIS.

6. Zarządzanie operacyjne systemem centralnym SIS obejmuje wszystkie zadania niezbędne do zapewnienia funkcjonowania systemu centralnego SIS zgodnie z niniejszym rozporządzeniem przez 24 godziny na dobę, 7 dni w tygodniu – w szczególności prace konserwacyjne oraz udoskonalenia techniczne niezbędne do sprawnego działania systemu. Zadania te obejmują również koordynowanie działań w zakresie testowania, zarządzanie tymi działaniami i ich wspieranie w odniesieniu do systemu centralnego SIS i N.SIS, zapewniające funkcjonowanie systemu centralnego SIS i N. SIS zgodnie z wymogami zgodności pod względem technicznym i funkcjonalnym określonymi w art. 9.

7. Komisja przyjmuje akty wykonawcze w celu określenia wymogów technicznych dotyczących infrastruktury łączności. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

Artykuł 16

Bezpieczeństwo – eu-LISA

1. W odniesieniu do systemu centralnego SIS i infrastruktury łączności eu-LISA przyjmuje niezbędne środki, obejmujące 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) uniemożliwić osobom nieuprawnionym dostęp do infrastruktury przetwarzania danych, wykorzystywanej do przetwarzania danych osobowych (kontrola dostępu do infrastruktury);

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

d) zapobiegać nieuprawnionemu wprowadzaniu danych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);

e) zapobiegać korzystaniu z systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników);

f) zapobiegać nieuprawnionemu przetwarzaniu danych w SIS oraz nieuprawnionemu zmienianiu lub usuwaniu danych przetwarzanych w SIS (kontrola wprowadzania danych);

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

h) stworzyć profile z opisem funkcji i zadań osób, które są uprawnione do dostępu do danych lub do infrastruktury przetwarzania danych, i niezwłocznie udostępniać te profile Europejskiemu Inspektorowi Ochrony Danych na jego wniosek (profile personelu);

i) zapewnić możliwość weryfikacji i stwierdzania, którym podmiotom można przesyłać dane osobowe za pośrednictwem sprzętu do przesyłu danych (kontrola przesyłu danych);

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

k) zapobiegać nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas transportu nośników danych, w szczególności poprzez zastosowanie odpowiednich technik szyfrowania (kontrola transportu);

l) monitorować skuteczność środków bezpieczeństwa, o których mowa w niniejszym ustępie, oraz stosować konieczne środki organizacyjne dotyczące monitorowania wewnętrznego, aby zapewnić przestrzeganie niniejszego rozporządzenia (kontrolowanie własnej działalności);

m) zapewnić w razie przerwy w działaniu możliwość przywrócenia normalnego funkcjonowania zainstalowanych systemów (odzyskiwanie);

n) zapewnić, by SIS wykonywał właściwie swoje funkcje, by błędy były zgłaszane (niezawodność) i by dane osobowe przechowywane w SIS nie mogły ulec uszkodzeniu w wyniku nieprawidłowego funkcjonowania systemu (integralność); oraz

o) zapewnić bezpieczeństwo swoich centrów technicznych.

2. eu-LISA stosuje środki równoważne środkom, o których mowa w ust. 1, w odniesieniu do bezpieczeństwa przetwarzania i wymiany informacji uzupełniających przy użyciu infrastruktury łączności.

Artykuł 17

Poufność – eu-LISA

1. Bez uszczerbku dla art. 17 regulaminu pracowniczego eu-LISA stosuje odpowiednie przepisy dotyczące tajemnicy zawodowej lub innych równoważnych obowiązków w zakresie poufności – o standardzie porównywalnym do tych ustanowionych w art. 11 niniejszego rozporządzenia – do wszystkich swoich pracowników, od których wymaga się pracy z danymi SIS. Wymóg ten ma zastosowanie również po zakończeniu pełnienia urzędu przez te osoby lub po ustaniu ich zatrudnienia lub po zakończeniu ich działalności.

2. eu-LISA stosuje środki równoważne środkom, o których mowa w ust. 1, w odniesieniu do poufności w zakresie wymiany informacji uzupełniających przy użyciu infrastruktury łączności.

3. W przypadku gdy eu-LISA współpracuje z wykonawcami zewnętrznymi przy zadaniach związanych z SIS, ściśle monitoruje ona działania wykonawcy, by zapewnić przestrzeganie wszelkich przepisów niniejszego rozporządzenia, w szczególności przepisów dotyczących bezpieczeństwa, poufności i ochrony danych.

4. Zarządzania operacyjnego CS-SIS nie powierza się przedsiębiorstwom prywatnym ani organizacjom prywatnym.

Artykuł 18

Prowadzenie rejestrów na szczeblu centralnym

1. eu-LISA zapewnia rejestrowanie każdego dostępu do danych osobowych w CS-SIS oraz wszelkiej wymiany takich danych w ramach CS-SIS w celach, o których mowa w art. 12 ust. 1.

2. Zapisy w rejestrze wskazują w szczególności historię wpisu, datę i godzinę przetwarzania danych, dane wykorzystane do wyszukiwania, odniesienie do przetwarzanych danych oraz indywidualne i niepowtarzalne identyfikatory użytkownika dotyczące właściwego organu przetwarzającego dane.

3. Na zasadzie odstępstwa od ust. 2 niniejszego artykułu, jeżeli wyszukiwanie przeprowadza się z wykorzystaniem danych daktyloskopijnych lub wizerunków twarzy zgodnie z art. 33, zapisy w rejestrze zamiast danych rzeczywistych wskazują rodzaj danych wykorzystanych do wyszukiwania.

4. Zapisy w rejestrze są wykorzystywane wyłącznie do celów, o których mowa w ust. 1, i są usuwane po upływie trzech lat od ich utworzenia. Zapisy w rejestrze obejmujące historię wpisów są usuwane po upływie trzech lat od usunięcia wpisów.

5. Zapisy w rejestrze mogą być przechowywane dłużej niż przez okresy, o których mowa w ust. 4, jeśli są niezbędne do dalszego prowadzenia procedur monitorowania, które już się rozpoczęły.

6. Do celów monitorowania własnej działalności i zapewnienia należytego działania CS-SIS oraz integralności i bezpieczeństwa danych eu-LISA ma dostęp do rejestrów w granicach swoich uprawnień.

Europejski Inspektor Ochrony Danych ma dostęp do tych rejestrów na swój wniosek, w granicach swoich uprawnień i na potrzeby wykonywania swoich zadań.

ROZDZIAŁ IV

INFORMOWANIE OPINII PUBLICZNEJ

Artykuł 19

Kampanie informacyjne dotyczące SIS

W momencie rozpoczęcia stosowania niniejszego rozporządzenia Komisja – we współpracy z organami nadzorczymi i Europejskim Inspektorem Ochrony Danych – przeprowadza kampanię informacyjną, w ramach której informuje opinię publiczną o celach SIS, danych przechowywanych w SIS, organach mających dostęp do SIS oraz prawach przysługujących osobom, których dane dotyczą. Komisja regularnie powtarza takie kampanie we współpracy z organami nadzorczymi i Europejskim Inspektorem Ochrony Danych. Komisja prowadzi ogólnodostępną stronę internetową poświęconą wszelkim stosownym informacjom związanym z SIS. Państwa członkowskie – we współpracy ze swoimi organami nadzorczymi – opracowują i wprowadzają w życie niezbędne strategie służące ogólnemu informowaniu obywateli i rezydentów o SIS.

ROZDZIAŁ V

WPISY DOTYCZĄCE ODMOWY WJAZDU I POBYTU DOTYCZĄCE OBYWATELI PAŃSTW TRZECICH

Artykuł 20

Kategorie danych

1. Bez uszczerbku dla art. 8 ust. 1 lub dla przepisów niniejszego rozporządzenia dotyczących przechowywania danych dodatkowych, SIS zawiera wyłącznie te kategorie danych dostarczanych przez każde państwo członkowskie, których wymagają cele określone w art. 24 i 25.

2. Każdy wpis w SIS, który zawiera informacje na temat osób, obejmuje wyłącznie następujące dane:

a) nazwiska;

b) imiona;

c) imiona i nazwiska nadane przy urodzeniu;

d) poprzednio używane imiona i nazwiska oraz pseudonimy;

e) wszelkie szczególne obiektywne cechy fizyczne niepodlegające zmianom;

f) miejsce urodzenia;

g) data urodzenia;

h) płeć;

i) wszelkie posiadane obywatelstwa;

j) informacje o tym, czy dana osoba:

   (i) jest uzbrojona;

   (ii) jest agresywna;

   (iii) ukryła się lub uciekła;

   (iv) wykazuje skłonności samobójcze;

   (v) stanowi zagrożenie dla zdrowia publicznego; lub

   (vi) jest zaangażowana w działalność, o której mowa w art. 3–14 dyrektywy (UE) 2017/541;

k) podstawa wpisu;

l) organ, który utworzył wpis;

m) odesłanie do decyzji będącej podstawą wpisu;

n) działanie, które należy podjąć w przypadku trafienia;

o) odsyłacze do innych wpisów zgodnie z art. 48;

p) informacje o tym, czy dana osoba jest członkiem rodziny obywatela Unii lub innej osoby, której przysługuje prawo do swobodnego przemieszczania się, o czym mowa w art. 26;

q) informacje o tym, czy podstawą decyzji o odmowie wjazdu i pobytu jest:

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

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

(iii) obejście unijnych lub krajowych przepisów dotyczących wjazdu i pobytu, o czym mowa w art. 24 ust. 2 lit. c);

(iv) zakaz wjazdu, o którym mowa w art. 24 ust. 1 lit. b); lub

(v) środek ograniczający, o którym mowa w art. 25;

r) rodzaj przestępstwa;

s) kategoria dokumentów identyfikacyjnych danej osoby;

t) państwo wydania dokumentów identyfikacyjnych danej osoby;

u) numer lub numery dokumentów identyfikacyjnych danej osoby;

v) data wydania dokumentów identyfikacyjnych danej osoby;

w) fotografie i wizerunki twarzy;

x) dane daktyloskopijne;

y) kopia, w miarę możliwości w kolorze, dokumentów identyfikacyjnych.

3. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów technicznych niezbędnych do wprowadzania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 2 niniejszego artykułu, a także wspólnych norm, o których mowa w ust. 4 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

4. Przepisy techniczne są podobne dla wyszukiwań w CS-SIS, w kopiach krajowych lub wspólnych kopiach oraz w kopiach technicznych sporządzanych na podstawie art. 41 ust. 2. Ich podstawę stanowią wspólne normy.

Artykuł 21

Proporcjonalność

1. Przed wprowadzeniem wpisu i przy przedłużeniu okresu ważności wpisu państwa członkowskie oceniają, czy dany przypadek jest wystarczająco adekwatny, odpowiedni i ważny, by uzasadnić wpis w SIS.

2. Jeżeli decyzja o odmowie wjazdu i pobytu, o której mowa w art. 24 ust. 1 lit. a), związana jest z przestępstwem terrorystycznym, dany przypadek uznaje się za wystarczająco adekwatny, odpowiedni i ważny, by uzasadnić wpis w SIS. Ze względu na bezpieczeństwo publiczne lub narodowe państwa członkowskie mogą wyjątkowo nie wprowadzać wpisu, jeśli istnieje prawdopodobieństwo, że utrudniłby on prowadzenie dochodzeń urzędowych lub sądowych, postępowań przygotowawczych lub innych postępowań.

Artykuł 22

Wymóg warunkujący wprowadzenie wpisu

1. Minimalny zestaw danych niezbędnych do wprowadzenia wpisu do SIS obejmuje dane, o których mowa w art. 20 ust. 2 lit. a), g), k), m), n) i q). Inne dane, o których mowa w tym ustępie, także wprowadza się do SIS, jeśli są dostępne.

2. Dane, o których mowa w art. 20 ust. 2 lit. e) niniejszego rozporządzenia, wprowadza się wyłącznie w przypadkach gdy jest to bezwzględnie niezbędne do identyfikacji danego obywatela państwa trzeciego. Jeżeli takie dane zostaną wprowadzone, państwa członkowskie zapewniają przestrzeganie art. 9 rozporządzenia (UE) 2016/679.

Artykuł 23

Zgodność wpisów

1. Przed wprowadzeniem wpisu państwo członkowskie sprawdza, czy w SIS istnieje już wpis dotyczący danej osoby. W tym celu przeprowadza się również sprawdzenie przy użyciu danych daktyloskopijnych, jeśli dane takie są dostępne.

2. Państwo członkowskie może wprowadzić do SIS tylko jeden wpis dotyczący danej osoby. W razie potrzeby inne państwa członkowskie mogą wprowadzić nowe wpisy dotyczące tej samej osoby, zgodnie z ust. 3.

3. Jeżeli istnieje już w SIS wpis dotyczący danej osoby, państwo członkowskie, które chce wprowadzić nowy wpis, sprawdza, czy między wpisami nie ma niezgodności. Jeżeli niezgodności nie ma, państwo członkowskie może wprowadzić nowy wpis. Jeżeli wpisy są ze sobą niezgodne, odpowiednie biura SIRENE państw członkowskich konsultują się ze sobą, dokonując wymiany informacji uzupełniających w celu osiągnięcia porozumienia. Zasady dotyczące zgodności wpisów określa się w podręczniku SIRENE. Po przeprowadzeniu między państwami członkowskimi konsultacji można odstąpić od zasad dotyczących zgodności wpisów z uwagi na istotny interes narodowy.

4. Jeżeli uzyskano trafienia w następstwie wielokrotnych wpisów dotyczących tej samej osoby, wykonujące państwo członkowskie przestrzega zasad dotyczących priorytetu poszczególnych wpisów, które to zasady określono w podręczniku SIRENE.

Jeżeli danej osoby dotyczą wielokrotne wpisy wprowadzone przez różne państwa członkowskie, w pierwszej kolejności wykonywane są wpisy mające doprowadzić do aresztowania wprowadzone zgodnie z art. 26 rozporządzenia (UE) 2018/1862, z zastrzeżeniem art. 25 tego rozporządzenia.

Artykuł 24

Warunki dokonywania wpisów dotyczących odmowy wjazdu i pobytu

1. Państwa członkowskie wprowadzają wpis dotyczący odmowy wjazdu i pobytu, jeżeli spełniony zostanie jeden z następujących warunków:

a) państwo członkowskie stwierdziło – na podstawie indywidualnej oceny, która obejmuje ocenę sytuacji osobistej danego obywatela państwa trzeciego i skutków odmowy mu wjazdu i pobytu – że obecność tego obywatela państwa trzeciego na jego terytorium stanowi zagrożenie dla porządku publicznego, bezpieczeństwa publicznego lub bezpieczeństwa narodowego i w związku z tym państwo członkowskie wydało zgodnie ze swoim prawem krajowym decyzję sądową lub administracyjną o odmowie wjazdu i pobytu oraz wprowadziło wpis krajowy dotyczący odmowy wjazdu i pobytu; lub

b) państwo członkowskie wydało w odniesieniu do obywatela państwa trzeciego zakaz wjazdu zgodnie z procedurami spełniającymi wymogi dyrektywy 2008/115/WE.

2. Sytuacje, o których mowa w ust. 1 lit. a), mają miejsce, gdy:

a) obywatel państwa trzeciego został skazany w jednym z państw członkowskich za przestępstwo zagrożone karą pozbawienia wolności wynoszącą co najmniej rok;

b) istnieją poważne podstawy, by sądzić, że obywatel państwa trzeciego popełnił poważne przestępstwo, w tym przestępstwo terrorystyczne, lub istnieją wyraźne przesłanki wskazujące, że zamierza on popełnić takie przestępstwo na terytorium jednego z państw członkowskich; lub

c) obywatel państwa trzeciego obszedł lub usiłował obejść przepisy prawa Unii lub prawa krajowego dotyczące wjazdu i pobytu na terytorium państw członkowskich.

3. Aby zapobiec ponownemu wjazdowi danego obywatela państwa trzeciego, państwo członkowskie dokonujące wpisu zapewnia, by wpis stawał się skuteczny w SIS w momencie, gdy dany obywatel państwa trzeciego opuszcza terytorium państw członkowskich lub niezwłocznie po stwierdzeniu przez państwo członkowskie dokonujące wpisu istnienia wyraźnych przesłanek wskazujących, że dany obywatel państwa trzeciego opuścił terytorium państw członkowskich.

4. Osoby, w odniesieniu do których wydano decyzję o odmowie wjazdu i pobytu, o której mowa w ust. 1, mają prawo wnieść odwołanie od tej decyzji. Takie postępowanie odwoławcze prowadzone jest zgodnie z prawem Unii i prawem krajowym, które musi przewidywać prawo do skutecznego środka ochrony przed sądem.

Artykuł 25

Warunki wprowadzania wpisów dotyczących obywateli państw trzecich, którzy są objęci środkami ograniczającymi

1. Wpisy dotyczące obywateli państw trzecich, którzy są objęci środkami ograniczającymi mającymi zapobiec wjazdowi na terytorium państw członkowskich lub przejazdowi przez to terytorium, podejmowanymi zgodnie z aktami prawnymi przyjętymi przez Radę, w tym środkami służącymi wykonaniu zakazu podróżowania wydanego przez Radę Bezpieczeństwa Organizacji Narodów Zjednoczonych, są wprowadzane do SIS na potrzeby odmowy wjazdu i pobytu, o ile spełnione są wymogi dotyczące jakości danych.

2. Wpisy wprowadza, aktualizuje i usuwa właściwy organ państwa członkowskiego, które w momencie przyjęcia danego środka sprawuje prezydencję w Radzie Unii Europejskiej. Jeżeli to państwo członkowskie nie ma dostępu do SIS lub do wpisów wprowadzonych zgodnie z niniejszym rozporządzeniem, obowiązek ten przejmuje państwo członkowskie, które ma sprawować kolejną prezydencję i które ma dostęp do SIS, w tym dostęp do wpisów wprowadzonych zgodnie z niniejszym rozporządzeniem.

Państwa członkowskie ustanawiają niezbędne procedury wprowadzania, aktualizowania i usuwania takich wpisów.

Artykuł 26

Warunki wprowadzania wpisów dotyczących obywateli państw trzecich, którym przysługuje prawo do swobodnego przemieszczania się w obrębie Unii

1. Wpis dotyczący obywatela państwa trzeciego, któremu przysługuje prawo do swobodnego przemieszczania się w obrębie Unii zgodnie z dyrektywą 2004/38/WE lub zgodnie z umową między Unią lub Unią i jej państwami członkowskimi, z jednej strony, a państwem trzecim, z drugiej – musi być zgodny z przepisami przyjętymi w ramach wdrożenia tej dyrektywy lub umowy.

2. W przypadku trafienia dotyczącego wpisu wprowadzonego zgodnie z art. 24 w odniesieniu do obywatela państwa trzeciego, któremu przysługuje prawo do swobodnego przemieszczania się w obrębie Unii, wykonujące państwo członkowskie natychmiast konsultuje się – w drodze wymiany informacji uzupełniających – z państwem członkowskim dokonującym wpisu, tak by niezwłocznie podjąć decyzję w sprawie działania, które należy podjąć.

Artykuł 27

Konsultacje przeprowadzane przed przyznaniem dokumentu pobytowego lub wizy długoterminowej lub przedłużeniem ich ważności

Jeżeli państwo członkowskie rozważa przyznanie dokumentu pobytowego lub wizy długoterminowej lub przedłużenie ich ważności obywatelowi państwa trzeciego, do którego odnosi się wpis dotyczący odmowy wjazdu i pobytu wprowadzony przez inne państwo członkowskie, zaangażowane państwa członkowskie konsultują się ze sobą, w drodze wymiany informacji uzupełniających, zgodnie z następującymi zasadami:

a) przed przyznaniem dokumentu pobytowego lub wizy długoterminowej lub przedłużeniem ich ważności przyznające państwo członkowskie konsultuje się z państwem członkowskim dokonującym wpisu;

b) państwo członkowskie dokonujące wpisu odpowiada na wniosek w sprawie konsultacji w terminie 10 dni kalendarzowych;

c) brak odpowiedzi w terminie, o którym mowa w lit. b), oznacza, że państwo członkowskie dokonujące wpisu nie sprzeciwia się przyznaniu lub przedłużeniu ważności dokumentu pobytowego lub wizy długoterminowej;

d) przy podejmowaniu odnośnej decyzji przyznające państwo członkowskie bierze pod uwagę powody leżące u podstaw decyzji państwa członkowskiego dokonującego wpisu oraz uwzględnia, zgodnie z prawem krajowym, zagrożenia dla porządku publicznego lub bezpieczeństwa publicznego, jakie może powodować obecność danego obywatela państwa trzeciego na terytorium państw członkowskich;

e) przyznające państwo członkowskie powiadamia o swojej decyzji państwo członkowskie dokonujące wpisu; oraz

f) jeżeli przyznające państwo członkowskie powiadomi państwo członkowskie dokonujące wpisu, że zamierza przyznać dokument pobytowy lub wizę długoterminową lub przedłużyć ich ważność lub że postanowiło to zrobić, państwo członkowskie dokonujące wpisu usuwa wpis dotyczący odmowy wjazdu i pobytu.

Ostateczna decyzja w sprawie tego, czy obywatelowi państwa trzeciego należy przyznać dokument pobytowy lub wizę długoterminową, należy do przyznającego państwa członkowskiego.

Artykuł 28

Konsultacje przeprowadzane przed wprowadzeniem wpisu dotyczącego odmowy wjazdu i pobytu

Jeżeli państwo członkowskie podjęło decyzję, o której mowa w art. 24 ust. 1, i rozważa wprowadzenie wpisu dotyczącego odmowy wjazdu i pobytu w odniesieniu do obywatela państwa trzeciego, który posiada ważny dokument pobytowy lub ważną wizę długoterminową przyznane przez inne państwo członkowskie, zaangażowane państwa członkowskie konsultują się ze sobą, w drodze wymiany informacji uzupełniających, zgodnie z następującymi zasadami:

a) państwo członkowskie, które podjęło decyzję, o której mowa w art. 24 ust. 1, informuje o tej decyzji przyznające państwo członkowskie;

b) wymiana informacji, o której mowa w lit. a) niniejszego artykułu, obejmuje wystarczające informacje o powodach leżących u podstaw decyzji, o której mowa w art. 24 ust. 1;

c) na podstawie informacji przedstawionych przez państwo członkowskie, które podjęło decyzję, o której mowa w art. 24 ust. 1, przyznające państwo członkowskie rozważa, czy istnieją powody do cofnięcia dokumentu pobytowego lub wizy długoterminowej;

d) przy podejmowaniu odnośnej decyzji przyznające państwo członkowskie bierze pod uwagę powody leżące u podstaw decyzji państwa członkowskiego, które podjęło decyzję, o której mowa w art. 24 ust. 1, oraz uwzględnia, zgodnie z prawem krajowym, zagrożenia dla porządku publicznego lub bezpieczeństwa publicznego, jakie może powodować obecność danego obywatela państwa trzeciego na terytorium państw członkowskich;

e) w terminie 14 dni kalendarzowych od otrzymania wniosku w sprawie konsultacji przyznające państwo członkowskie powiadamia państwo członkowskie, które podjęło decyzję, o której mowa w art. 24 ust. 1, o swojej decyzji lub, jeśli podjęcie decyzji w tym terminie przez przyznające państwo członkowskie nie było możliwe, składa umotywowany wniosek o przedłużenie w drodze wyjątku terminu na udzielenie odpowiedzi o maksymalnie 12 dni kalendarzowych;

f) jeżeli przyznające państwo członkowskie powiadomi państwo członkowskie, które podjęło decyzję, o której mowa w art. 24 ust. 1, że utrzymuje w mocy dokument pobytowy lub wizę długoterminową, państwo członkowskie, które podjęło tę decyzję, nie wprowadza wpisu dotyczącego odmowy wjazdu i pobytu.

Artykuł 29

Konsultacje przeprowadzane po wprowadzeniu wpisu dotyczącego odmowy wjazdu i pobytu

Jeśli okaże się, że państwo członkowskie wprowadziło wpis dotyczący odmowy wjazdu i pobytu w odniesieniu do obywatela państwa trzeciego, który posiada ważny dokument pobytowy lub ważną wizę długoterminową przyznane przez inne państwo członkowskie, zaangażowane państwa członkowskie konsultują się ze sobą, w drodze wymiany informacji uzupełniających, zgodnie z następującymi zasadami:

a) państwo członkowskie dokonujące wpisu informuje przyznające państwo członkowskie o wpisie dotyczącym odmowy wjazdu i pobytu;

b) informacje wymieniane zgodnie z lit. a) obejmują wystarczające informacje o powodach wpisu dotyczącego odmowy wjazdu i pobytu;

c) na podstawie informacji przekazanych przez państwo członkowskie dokonujące wpisu przyznające państwo członkowskie rozważa, czy istnieją powody do cofnięcia dokumentu pobytowego lub wizy długoterminowej;

d) przy podejmowaniu odnośnej decyzji przyznające państwo członkowskie bierze pod uwagę powody leżące u podstaw decyzji państwa członkowskiego dokonującego wpisu oraz uwzględnia, zgodnie z prawem krajowym, zagrożenia dla porządku publicznego lub bezpieczeństwa publicznego, jakie może powodować obecność danego obywatela państwa trzeciego na terytorium państw członkowskich;

e) w terminie 14 dni kalendarzowych od otrzymania wniosku w sprawie konsultacji przyznające państwo członkowskie powiadamia o swojej decyzji państwo członkowskie dokonujące wpisu lub, jeśli podjęcie decyzji w tym terminie przez przyznające państwo członkowskie nie było możliwe, składa umotywowany wniosek o przedłużenie terminu na udzielenie odpowiedzi o maksymalnie 12 dni kalendarzowych;

f) jeżeli przyznające państwo członkowskie powiadomi państwo członkowskie dokonujące wpisu, że utrzymuje w mocy dokument pobytowy lub wizę długoterminową, państwo członkowskie dokonujące wpisu natychmiast usuwa wpis dotyczący odmowy wjazdu i pobytu.

Artykuł 30

Konsultacje w przypadku trafienia odnoszącego się do obywatela państwa trzeciego, który posiada ważny dokument pobytowy lub ważną wizę długoterminową

Jeżeli państwo członkowskie uzyskuje trafienie odnoszące się do wpisu dotyczącego odmowy wjazdu i pobytu wprowadzonego przez jedno z państw członkowskich w odniesieniu do obywatela państwa trzeciego, który posiada ważny dokument pobytowy lub ważną wizę długoterminową przyznane przez inne państwo członkowskie, zaangażowane państwa członkowskie przeprowadzają konsultacje poprzez wymianę informacji uzupełniających zgodnie z następującymi zasadami:

a) wykonujące państwo członkowskie informuje o tej sytuacji państwo członkowskie dokonujące wpisu;

b) państwo członkowskie dokonujące wpisu wszczyna procedurę określoną w art. 29;

c) państwo członkowskie dokonujące wpisu powiadamia wykonujące państwo członkowskie o wyniku tych konsultacji.

Decyzja w sprawie wjazdu obywatela państwa trzeciego jest podejmowana przez wykonujące państwo członkowskie zgodnie z rozporządzeniem (UE) 2016/399.

Artykuł 31

Statystyki dotyczące wymiany informacji

Państwa członkowskie raz w roku przekazują eu-LISA statystyki dotyczące wymian informacji przeprowadzonych zgodnie z art. 27–30 oraz przypadków niedotrzymania terminów określonych w tych artykułach.

ROZDZIAŁ VI

WYSZUKIWANIE PRZY UŻYCIU DANYCH BIOMETRYCZNYCH

Artykuł 32

Przepisy szczegółowe dotyczące wprowadzania fotografii, wizerunków twarzy i danych daktyloskopijnych

1. Do SIS wprowadzane są wyłącznie fotografie, wizerunki twarzy i dane daktyloskopijne, o których mowa w art. 20 ust. 2 lit. w) oraz x), spełniające minimalne normy i specyfikacje techniczne dotyczące jakości danych. Przed wprowadzeniem takich danych przeprowadza się kontrolę jakości w celu ustalenia, czy spełniają one minimalne normy i specyfikacje techniczne dotyczące jakości danych.

2. Dane daktyloskopijne wprowadzane do SIS mogą składać się z jednej do dziesięciu płaskich odbitek linii papilarnych palców i jednej do dziesięciu przetoczonych odbitek linii papilarnych palców. Mogą one również zawierać do dwóch odbitek linii papilarnych dłoni.

3. Ustanawia się minimalne normy i specyfikacje techniczne dotyczące jakości danych zgodnie z ust. 4 niniejszego artykułu w odniesieniu do przechowywania danych biometrycznych, o których mowa w ust. 1 niniejszego artykułu. Te minimalne normy i specyfikacje techniczne dotyczące jakości danych określają poziom jakości wymagany do wykorzystywania danych w celu weryfikacji tożsamości osoby zgodnie z art. 33 ust. 1 i do wykorzystywania danych w celu zidentyfikowania osoby zgodnie z art. 33 ust. 2–4.

4. Komisja przyjmuje akty wykonawcze w celu ustanowienia minimalnych norm i specyfikacji technicznych dotyczących jakości danych, o których mowa w ust. 1 i 3 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

Artykuł 33

Przepisy szczegółowe dotyczące weryfikacji lub wyszukiwania przy użyciu fotografii, wizerunków twarzy i danych daktyloskopijnych

1. Jeżeli fotografie, wizerunki twarzy i dane daktyloskopijne są dostępne we wpisie w SIS, takie fotografie, wizerunki twarzy i dane daktyloskopijne wykorzystuje się w celu potwierdzenia tożsamości osoby, która została zlokalizowana w wyniku wyszukiwania alfanumerycznego przeprowadzonego w SIS.

2. Wyszukiwanie przy użyciu danych daktyloskopijnych może być przeprowadzone we wszystkich przypadkach w celu identyfikacji danej osoby. Jeżeli jednak tożsamości danej osoby nie można ustalić w żaden inny sposób, w celu identyfikacji przeprowadza się wyszukiwanie przy użyciu danych daktyloskopijnych. W tym celu system centralny SIS posiada Automatyczny System Identyfikacji Daktyloskopijnej.

3. Dane daktyloskopijne w SIS związane z wpisami wprowadzonymi na podstawie art. 24 i 25 można wyszukiwać również przy użyciu kompletnych lub niekompletnych zestawów odbitek linii papilarnych palców lub odbitek linii papilarnych dłoni, które znaleziono na miejscu popełnienia poważnych przestępstw lub przestępstw terrorystycznych będących przedmiotem postępowania przygotowawczego i w przypadku których z dużym prawdopodobieństwem można stwierdzić, że te zestawy odbitek linii papilarnych należą do sprawcy danego przestępstwa, pod warunkiem że wyszukiwanie przeprowadzane jest równolegle w odpowiednich bazach danych państwa członkowskiego zawierających odbitki linii papilarnych palców.

4. Gdy tylko stanie się to technicznie możliwe oraz przy jednoczesnym zapewnieniu wysokiego stopnia wiarygodności identyfikacji, można będzie wykorzystywać fotografie i wizerunki twarzy do identyfikacji danej osoby na stałych przejściach granicznych.

Zanim funkcja ta zostanie wdrożona w SIS, Komisja przedstawi sprawozdanie dotyczące dostępności, gotowości i niezawodności wymaganych rozwiązań technologicznych. Sprawozdanie to zostanie skonsultowane z Parlamentem Europejskim.

Po tym, jak funkcja ta zacznie być wykorzystywana na stałych przejściach granicznych, Komisja będzie uprawniona do przyjęcia aktów delegowanych zgodnie z art. 61 w celu uzupełnienia niniejszego rozporządzenia w zakresie określenia innych warunków, w których fotografie i wizerunki twarzy mogą być wykorzystywane do identyfikacji osób.

ROZDZIAŁ VII

PRAWO DO DOSTĘPU I WERYFIKACJA ORAZ USUWANIE WPISÓW

Artykuł 34

Właściwe organy krajowe mające prawo do dostępu do danych w SIS

1. Właściwe organy krajowe odpowiedzialne za identyfikację obywateli państw trzecich mają dostęp do danych wprowadzonych do SIS oraz prawo do wyszukiwania takich danych bezpośrednio lub w kopii bazy danych SIS do celów:

a) kontroli granicznej, zgodnie z rozporządzeniem (UE) 2016/399;

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

c) zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych lub ich ścigania lub wykonywania kar w danym państwie członkowskim, o ile zastosowanie ma dyrektywa (UE) 2016/680;

d) badania warunków i podejmowania decyzji dotyczących wjazdu i pobytu obywateli państw trzecich na terytorium państw członkowskich, w tym dokumentów pobytowych i wiz długoterminowych, oraz dotyczących powrotu obywateli państw trzecich, jak również przeprowadzania kontroli obywateli państw trzecich, którzy nielegalnie wjeżdżają lub przebywają na terytorium państw członkowskich;

e) kontroli bezpieczeństwa w odniesieniu do obywateli państw trzecich, którzy ubiegają się o ochronę międzynarodową, o ile organy przeprowadzające takie kontrole nie są „organami rozstrzygającymi" zdefiniowanymi w art. 2 lit. f) dyrektywy Parlamentu Europejskiego i Rady 2013/32/UE ([1]), oraz w stosownych przypadkach do celów wydawania opinii zgodnie z rozporządzeniem Rady (WE) nr 377/2004 ([2]);

f) rozpatrywania wniosków wizowych i podejmowania decyzji w sprawie tych wniosków, w tym decyzji o unieważnieniu, cofnięciu wiz lub przedłużeniu okresu ważności wiz, zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 810/2009 ([3]).

2. Prawo do dostępu do danych w SIS oraz prawo do bezpośredniego wyszukiwania takich danych może być wykonywane przez właściwe organy krajowe odpowiedzialne za naturalizację, określone w prawie krajowym, do celów rozpatrywania wniosków o naturalizację.

3. Na użytek art. 24 i 25 prawo do dostępu do danych w SIS oraz prawo do bezpośredniego wyszukiwania takich danych może być wykonywane również przez krajowe organy wymiaru sprawiedliwości, w tym organy odpowiedzialne za wszczynanie postępowań karnych z oskarżenia publicznego i prowadzenie postępowań przygotowawczych przed wniesieniem aktu oskarżenia, w ramach wykonywania ich zadań określonych w prawie krajowym, a także przez organy koordynujące ich działania.

4. Prawo do dostępu do danych dotyczących dokumentów odnoszących się do osób, które to dane wprowadzono zgodnie z art. 38 ust. 2 lit. k) i l) rozporządzenia (UE) 2018/1862, oraz prawo do wyszukiwania takich danych może być wykonywane również przez organy, o których mowa w ust. 1 lit. f) niniejszego artykułu.

5. Właściwe organy, o których mowa w niniejszym artykule, są uwzględniane w wykazie, o którym mowa w art. 41 ust. 8.

Artykuł 35

Dostęp Europolu do danych w SIS

1. Jeżeli jest to niezbędne do wykonywania jej mandatu, Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), ustanowiona rozporządzeniem (UE) 2016/794, ma prawo do dostępu do danych w SIS i do ich wyszukiwania. Europol może też dokonywać wymiany informacji uzupełniających i występować z wnioskami o dalsze informacje uzupełniające zgodnie z zasadami zawartymi w podręczniku SIRENE.

2. Jeżeli podczas wyszukiwania Europol stwierdzi istnienie wpisu w SIS, informuje o tym – w drodze wymiany informacji uzupełniających przy użyciu infrastruktury łączności i zgodnie z zasadami zawartymi w podręczniku SIRENE – państwo członkowskie dokonujące wpisu. Dopóki Europol nie będzie w stanie korzystać z funkcji przewidzianych do wymiany informacji uzupełniających, w celu przekazywania informacji państwom członkowskim dokonującym wpisu wykorzystuje kanały określone w rozporządzeniu (UE) 2016/794.

3. Europol może przetwarzać informacje uzupełniające, które przekazały mu państwa członkowskie, do celów przeprowadzania porównań ze swoimi bazami danych i projektami analitycznymi, mających służyć wskazaniu powiązań lub innych odpowiednich związków, oraz do celów analiz strategicznych, tematycznych lub operacyjnych, o których mowa w art. 18 ust. 2 lit. a), b) i c) rozporządzenia (UE) 2016/794. Europol przetwarza informacje uzupełniające do celów niniejszego artykułu zgodnie z tym rozporządzeniem.

4. Wykorzystanie przez Europol informacji uzyskanych w wyniku wyszukiwania w SIS lub w wyniku przetwarzania informacji uzupełniających wymaga zgody państwa członkowskiego dokonującego wpisu. Jeżeli to państwo członkowskie zezwoli na wykorzystanie takich informacji, posługiwanie się nimi przez Europol regulowane jest rozporządzeniem (UE) 2016/794. Europol przekazuje takie informacje państwom trzecim i podmiotom trzecim wyłącznie za zgodą państwa członkowskiego dokonującego wpisu i z pełnym poszanowaniem prawa Unii dotyczącego ochrony danych.

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2013/32/UE z dnia 26 czerwca 2013 r. w sprawie wspólnych procedur udzielania i cofania ochrony międzynarodowej (Dz.U. L 180 z 29.6.2013, s. 60).

([2]) Rozporządzenie Rady (WE) nr 377/2004 z dnia 19 lutego 2004 r. w sprawie utworzenia sieci oficerów łącznikowych ds. imigracji (Dz.U. L 64 z 2.3.2004, s. 1).

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

5. Europol:

a) bez uszczerbku dla ust. 4 i 6 nie podłącza części SIS ani nie przekazuje danych, które są w tych częściach zawarte i do których ma dostęp, do systemu gromadzenia i przetwarzania danych stosowanego przez Europol lub w Europolu, a także nie pobiera ani w inny sposób nie kopiuje części SIS;

b) niezależnie od art. 31 ust. 1 rozporządzenia (UE) 2016/794 usuwa informacje uzupełniające zawierające dane osobowe najpóźniej rok po usunięciu związanego z nimi wpisu. Na zasadzie odstępstwa, jeżeli Europol posiada w swoich bazach danych lub projektach analitycznych informacje o sprawie, której dotyczą informacje uzupełniające, w celu wykonywania swoich zadań Europol może wyjątkowo w razie potrzeby nadal przechowywać te informacje uzupełniające. Europol informuje państwo członkowskie dokonujące wpisu i wykonujące państwo członkowskie o dalszym przechowywaniu takich informacji uzupełniających i przedstawia jego uzasadnienie;

c) ogranicza dostęp do danych w SIS, w tym do informacji uzupełniających, tak by korzystali z niego tylko specjalnie uprawnieni pracownicy Europolu, którym dostęp do takich danych jest potrzebny do wykonywania ich zadań;

d) przyjmuje i stosuje środki służące zapewnieniu bezpieczeństwa, poufności i monitorowania własnej działalności zgodnie z art. 10, 11 i 13;

e) zapewnia, by pracownicy uprawnieni do przetwarzania danych SIS przeszli odpowiednie szkolenie i zostali odpowiednio poinformowani zgodnie z art. 14 ust. 1; oraz

f) bez uszczerbku dla rozporządzenia (UE) 2016/794 zapewnia Europejskiemu Inspektorowi Ochrony Danych możliwość monitorowania i kontrolowania działań podejmowanych przez Europol w ramach wykonywania prawa do dostępu do danych w SIS i ich wyszukiwania oraz w ramach wymiany i przetwarzania informacji uzupełniających.

6. Europol kopiuje dane z SIS wyłącznie do celów technicznych, jeżeli takie kopiowanie jest niezbędne do przeprowadzenia bezpośredniego wyszukiwania przez należycie uprawnionych pracowników Europolu. Do takich kopii zastosowanie ma niniejsze rozporządzenie. Kopię techniczną wykorzystuje się wyłącznie do przechowywania danych SIS w trakcie przeprowadzania ich wyszukiwania. Po przeprowadzeniu wyszukiwania danych dane te są usuwane. Takich przypadków wykorzystywania danych nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie danych SIS. Europol nie kopiuje do innych systemów Europolu danych zawartych we wpisach lub danych dodatkowych wprowadzonych przez państwa członkowskie lub pochodzących z CS-SIS.

7. Do celów weryfikacji zgodności przetwarzania danych z prawem, monitorowania własnej działalności oraz zapewniania należytego bezpieczeństwa i integralności danych Europol rejestruje zgodnie z przepisami art. 12 każdy dostęp do SIS oraz każde wyszukiwanie w SIS. Prowadzenia takiej rejestracji i dokumentacji nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie części SIS.

8. Państwa członkowskie informują Europol w drodze wymiany informacji uzupełniających o każdym trafieniu odnoszącym się do wpisów dotyczących przestępstw terrorystycznych. Państwa członkowskie mogą w wyjątkowych okolicznościach nie przekazywać Europolowi takich informacji, jeżeli takie przekazanie mogłoby spowodować zagrożenie dla realizowanych czynności lub bezpieczeństwa osób lub byłoby sprzeczne z istotnymi interesami w zakresie bezpieczeństwa państwa członkowskiego dokonującego wpisu.

9. Ust. 8 stosuje się od daty, z którą Europol będzie w stanie otrzymywać informacje uzupełniające zgodnie z ust. 1.

Artykuł 36

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

1. Zgodnie z art. 40 ust. 8 rozporządzenia (UE) 2016/1624 członkowie zespołów, o których mowa w art. 2 pkt 8 i 9 tego rozporządzenia, mają – w ramach swojego mandatu oraz pod warunkiem że są uprawnieni do przeprowadzania kontroli zgodnie z art. 34 ust. 1 niniejszego rozporządzenia i przeszli wymagane szkolenie zgodnie z art. 14 ust. 1 niniejszego rozporządzenia – prawo do dostępu do danych w SIS oraz do wyszukiwania takich danych w zakresie, w jakim jest to niezbędne do wykonywania ich zadań i zgodnie z wymogami planu operacyjnego dla danej operacji. Inni członkowie zespołów nie są uprawnieni do dostępu do danych w SIS.

2. Członkowie zespołów, o których mowa w ust. 1, wykonują prawo do dostępu do danych w SIS oraz do wyszukiwania takich danych zgodnie z ust. 1, korzystając z interfejsu technicznego. Interfejs techniczny zostanie utworzony i będzie prowadzony przez Europejską Agencję Straży Granicznej i Przybrzeżnej i będzie umożliwiał bezpośrednie połączenie z systemem centralnym SIS.

3. Jeżeli w wyniku wyszukiwania członek zespołów, o których mowa w ust. 1 niniejszego artykułu, stwierdzi istnienie wpisu w SIS, powiadamia się o tym fakcie państwo członkowskie dokonujące wpisu. Zgodnie z art. 40 rozporządzenia (UE) 2016/1624 członkowie zespołów podejmują działania w odpowiedzi na wpis w SIS wyłącznie na polecenie i – co do zasady – w obecności funkcjonariuszy straży granicznej lub personelu realizującego zadania w dziedzinie powrotów z przyjmującego państwa członkowskiego, w którym działają. Przyjmujące państwo członkowskie może upoważnić członków zespołów do działania w jego imieniu.

4. Do celów weryfikacji zgodności przetwarzania danych z prawem, monitorowania własnej działalności oraz zapewniania należytego bezpieczeństwa i integralności danych Europejska Agencja Straży Granicznej i Przybrzeżnej rejestruje zgodnie z przepisami art. 12 każdy dostęp do SIS oraz każde wyszukiwanie w SIS.

5. Europejska Agencja Straży Granicznej i Przybrzeżnej przyjmuje i stosuje środki służące zapewnieniu bezpieczeństwa, poufności i monitorowania własnej działalności zgodnie z art. 10, 11 i 13 oraz zapewnia, by zespoły, o których mowa w ust. 1 niniejszego artykułu, stosowały te środki.

6. Przepisów niniejszego artykułu nie można interpretować jako mających wpływ na przepisy rozporządzenia (UE) 2016/1624 dotyczące ochrony danych i odpowiedzialności za nieuprawnione lub nieprawidłowe przetwarzanie danych przez Europejską Agencję Straży Granicznej i Przybrzeżnej.

7. Bez uszczerbku dla ust. 2 żadnych części SIS nie podłącza się do systemu gromadzenia i przetwarzania danych stosowanego przez zespoły, o których mowa w ust. 1, lub przez Europejską Agencję Straży Granicznej i Przybrzeżnej, a danych w SIS, do których dostęp mają te zespoły, nie przekazuje się do takiego systemu. Nie można pobierać ani kopiować żadnych części SIS. Rejestrowania dostępu i wyszukiwania nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie danych SIS.

8. Europejska Agencja Straży Granicznej i Przybrzeżnej zapewnia Europejskiemu Inspektorowi Ochrony Danych możliwość monitorowania i kontrolowania działań prowadzonych przez zespoły, o których mowa w niniejszym artykule, w ramach wykonywania ich prawa do dostępu do danych w SIS i wyszukiwania takich danych. Pozostaje to bez uszczerbku dla dalszych przepisów rozporządzenia (UE) 2018/1725.

Artykuł 37

Ocena użytkowania SIS przez Europol oraz Europejską Agencję Straży Granicznej i Przybrzeżnej

1. Co najmniej raz na pięć lat Komisja przeprowadza ocenę eksploatowania i użytkowania SIS przez Europol oraz zespoły, o których mowa w art. 36 ust. 1.

2. Europol i Europejska Agencja Straży Granicznej i Przybrzeżnej zapewniają podjęcie odpowiednich działań następczych w związku z ustaleniami i zaleceniami wynikającymi z tej oceny.

3. Sprawozdanie na temat wyników oceny i podjętych działań następczych przekazuje się Parlamentowi Europejskiemu i Radzie.

Artykuł 38

Zakres dostępu

Użytkownicy końcowi, w tym Europol i członkowie zespołów, o których mowa w art. 2 pkt 8 i 9 rozporządzenia (UE) 2016/1624, mają dostęp wyłącznie do tych danych, które są im niezbędne do wykonywania ich zadań.

Artykuł 39

Termin weryfikacji wpisów

1. Wpisy utrzymywane są wyłącznie przez czas konieczny do osiągnięcia celów, do których zostały wprowadzone.

2. W terminie trzech lat od wprowadzenia wpisu do SIS państwo członkowskie dokonujące wpisu weryfikuje, czy istnieje potrzeba jego dalszego utrzymywania. Jednakże jeżeli decyzja krajowa, która jest podstawą wpisu, przewiduje okres ważności dłuższy niż trzy lata, wpis weryfikuje się w terminie pięciu lat.

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

4. Przed upływem terminu weryfikacji państwo członkowskie dokonujące wpisu może, na podstawie wszechstronnej indywidualnej oceny, która podlega zarejestrowaniu, podjąć decyzję o utrzymaniu wpisu po upływie terminu weryfikacji, jeżeli jest to niezbędne i proporcjonalne do celów, do których wprowadzono ten wpis. W takim przypadku ust. 2 ma zastosowanie również do przedłużenia okresu utrzymywania wpisu. Informacje o takim przedłużeniu okresu utrzymywania wpisu są przekazywane do CS-SIS.

5. Po upływie terminu weryfikacji, o którym mowa w ust. 2, wpisy usuwane są automatycznie, z wyjątkiem przypadków, gdy państwo członkowskie dokonujące wpisu poinformowało CS-SIS o przedłużeniu okresu utrzymywania wpisu zgodnie z ust. 4. CS-SIS automatycznie informuje państwa członkowskie dokonujące wpisu z czteromiesięcznym wyprzedzeniem o zaplanowanym usunięciu danych.

6. Państwa członkowskie prowadzą statystyki na temat liczby wpisów, w odniesieniu do których okres utrzymywania został przedłużony zgodnie z ust. 4 niniejszego artykułu, i przekazują je organom nadzorczym, o których mowa w art. 55, na ich wniosek.

7. Jak tylko dla biura SIRENE stanie się jasne, że wpis spełnił swój cel i powinien w związku z tym zostać usunięty, natychmiast powiadamia ono o tym organ, który utworzył wpis. W terminie 15 dni kalendarzowych od otrzymania takiego powiadomienia organ ten informuje, że wpis został usunięty lub ma zostać usunięty, lub przedstawia powody dalszego utrzymywania wpisu. Jeżeli organ nie udzieli odpowiedzi w terminie 15 dni, biuro SIRENE zapewnia, by wpis został usunięty. Jeżeli jest to dopuszczalne na mocy prawa krajowego, wpis jest usuwany przez biuro SIRENE. Biura SIRENE zgłaszają swojemu organowi nadzorczemu powtarzające się problemy, które napotkały działając na podstawie niniejszego ustępu.

Artykuł 40

Usuwanie wpisów

1. Wpisy dotyczące odmowy wjazdu i pobytu na podstawie z art. 24 usuwa się:

a) gdy decyzja, na podstawie której wprowadzono wpis, została cofnięta przez właściwy organ lub właściwy organ stwierdził jej nieważność; lub

b) w stosownych przypadkach po przeprowadzeniu procedury konsultacji, o której mowa w art. 27 i 29.

2. Wpisy dotyczące obywateli państw trzecich, którzy są objęci środkiem ograniczającym mającym zapobiec wjazdowi na terytorium państw członkowskich lub przejazdowi przez to terytorium, są usuwane, gdy środek ograniczający przestanie obowiązywać lub gdy zostanie zawieszony lub gdy zostanie stwierdzona jego nieważność.

3. Wpisy dotyczące osoby, która nabyła obywatelstwo państwa członkowskiego lub jednego z państw, których obywatelom przysługuje prawo do swobodnego przemieszczania się na mocy prawa Unii, są usuwane, jak tylko państwo członkowskie dokonujące wpisu stwierdzi, że dana osoba nabyła takie obywatelstwo, lub uzyska informację na ten temat zgodnie z art. 44.

4. Wpisy są usuwane po wygaśnięciu wpisu zgodnie z art. 39.

ROZDZIAŁ VIII

PRZEPISY OGÓLNE DOTYCZĄCE PRZETWARZANIA DANYCH

Artykuł 41

Przetwarzanie danych SIS

1. Państwa członkowskie przetwarzają dane, o których mowa w art. 20, wyłącznie do celów odmowy wjazdu i pobytu na ich terytorium.

2. Dane mogą być kopiowane wyłącznie do celów technicznych, jeżeli takie kopiowanie jest niezbędne do przeprowadzenia bezpośredniego wyszukiwania przez właściwe organy, o których mowa w art. 34. Do takich kopii zastosowanie ma niniejsze rozporządzenie. Państwo członkowskie nie kopiuje – do innych krajowych plików danych – danych zawartych we wpisach ani danych dodatkowych wprowadzonych przez inne państwo członkowskie z N.SIS tego państwa lub z CS-SIS.

3. Kopie techniczne, o których mowa w ust. 2, przekształcane w bazy danych działające w trybie offline mogą być przechowywane przez okres nieprzekraczający 48 godzin.

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

Państwa członkowskie prowadzą aktualny spis takich kopii, który udostępniają swoim organom nadzorczym, oraz zapewniają, by w odniesieniu do tych kopii stosowane było niniejsze rozporządzenie, w szczególności art. 10.

4. Właściwe organy krajowe, o których mowa w art. 34, uzyskują dostęp do danych w SIS wyłącznie w granicach swoich kompetencji i jest on przyznawany wyłącznie należycie uprawnionym pracownikom.

5. Każdy przypadek przetwarzania przez państwa członkowskie danych SIS do celów innych niż te, w których informacje te zostały wprowadzone do SIS, musi być związany z konkretną sprawą i uzasadniony potrzebą zapobieżenia bezpośredniemu poważnemu zagrożeniu dla porządku publicznego i bezpieczeństwa publicznego, poważnymi względami bezpieczeństwa narodowego lub koniecznością zapobieżenia poważnemu przestępstwu. W tym celu uprzednio uzyskuje się zgodę państwa członkowskiego dokonującego wpisu.

6. Dane dotyczące dokumentów odnoszących się do osób wprowadzone do SIS zgodnie z art. 38 ust. 2 lit. k) i l) rozporządzenia (UE) 2018/1862 mogą być wykorzystywane przez właściwe organy, o których mowa w art. 34 ust. 1 lit. f), zgodnie z prawem każdego państwa członkowskiego.

7. Każdy przypadek wykorzystania danych SIS w sposób niezgodny z ust. 1–6 niniejszego artykułu uznaje się za wykorzystanie tych danych niezgodnie z przeznaczeniem w świetle prawa krajowego poszczególnych państw członkowskich i podlega on sankcjom zgodnie z art. 59.

8. Każde państwo członkowskie przekazuje eu-LISA wykaz swoich właściwych organów, które są uprawnione do przeprowadzania bezpośredniego wyszukiwania danych w SIS zgodnie z niniejszym rozporządzeniem, jak również wszelkie zmiany dotyczące tego wykazu. Wykaz ten określa – w odniesieniu do każdego organu – jakie dane mogą być wyszukiwane i w jakich celach. eu-LISA zapewnia coroczną publikację wykazu w *Dzienniku Urzędowym Unii Europejskiej*. eu-LISA prowadzi na swojej stronie internetowej stale aktualizowany wykaz zawierający zmiany przekazane przez państwa członkowskie w okresie pomiędzy corocznymi publikacjami.

9. Jeżeli prawo Unii nie zawiera przepisów szczegółowych, do danych w N.SIS zastosowanie mają przepisy poszczególnych państw członkowskich.

Artykuł 42

Dane SIS i pliki krajowe

1. Art. 41 ust. 2 pozostaje bez uszczerbku dla prawa państwa członkowskiego do utrzymywania w swoich plikach krajowych danych SIS, w związku z którymi podjęto działanie na jego terytorium. Takie dane są utrzymywane w plikach krajowych przez okres nie dłuższy niż trzy lata, chyba że przepisy szczegółowe prawa krajowego przewidują dłuższy okres ich utrzymywania.

2. Art. 41 ust. 2 pozostaje bez uszczerbku dla prawa państwa członkowskiego do utrzymywania w swoich plikach krajowych danych zawartych w konkretnym wpisie wprowadzonym do SIS przez to państwo członkowskie.

Artykuł 43

Poinformowanie o niewykonywaniu wpisu

Jeżeli wymagane działanie nie może zostać wykonane, wezwane do działania państwo członkowskie natychmiast informuje o tym – w drodze wymiany informacji uzupełniających – państwo członkowskie dokonujące wpisu.

Artykuł 44

Jakość danych w SIS

1. Państwo członkowskie dokonujące wpisu odpowiada za zapewnienie, by dane były prawidłowe, aktualne i wprowadzane do SIS oraz przechowywane w SIS zgodnie z prawem.

2. Jeżeli państwo członkowskie dokonujące wpisu uzyska odpowiednie dodatkowe lub zmienione dane wymienione w art. 20 ust. 2, niezwłocznie uzupełnia lub zmienia odnośny wpis.

3. Do zmiany, uzupełniania, korekty, aktualizacji lub usuwania danych wprowadzonych do SIS uprawnione jest wyłącznie państwo członkowskie dokonujące wpisu.

4. Jeżeli państwo członkowskie inne niż państwo członkowskie dokonujące wpisu posiada stosowne dodatkowe lub zmienione dane wymienione w art. 20 ust. 2, niezwłocznie przekazuje je – w drodze wymiany informacji uzupełniających – państwu członkowskiemu dokonującemu wpisu, tak by mogło ono uzupełnić lub zmienić wpis. Dane przekazywane są wyłącznie w przypadkach gdy tożsamość danego obywatela państwa trzeciego została ustalona.

5. Jeżeli państwo członkowskie inne niż państwo dokonujące wpisu posiada dowody wskazujące, że jeden z elementów danych jest niezgodny ze stanem faktycznym lub jest przechowywany niezgodnie z prawem, informuje o tym – w drodze wymiany informacji uzupełniających – państwo członkowskie dokonujące wpisu, jak najszybciej i nie później niż dwa dni robocze po stwierdzeniu istnienia takich dowodów. Państwo członkowskie dokonujące wpisu sprawdza te informacje oraz, w razie konieczności, niezwłocznie koryguje lub usuwa zakwestionowany element danych.

6. Jeżeli państwa członkowskie nie są w stanie osiągnąć porozumienia w terminie dwóch miesięcy od stwierdzenia istnienia dowodów, o których mowa w ust. 5 niniejszego artykułu, państwo członkowskie, które nie wprowadziło wpisu, przekazuje sprawę w drodze współpracy zgodnie z art. 57 odpowiednim krajowym organom nadzorczym i Europejskiemu Inspektorowi Ochrony Danych, którzy podejmują decyzję.

7. Jeżeli dana osoba twierdzi, że nie jest osobą, której ma dotyczyć wpis, państwa członkowskie przeprowadzają wymianę informacji uzupełniających. Jeżeli w wyniku sprawdzenia okaże się, że wnoszący skargę nie jest osobą, której ma dotyczyć wpis, zostaje on powiadomiony o środkach określonych w art. 47 i o przysługującym mu środku ochrony prawnej zgodnie z art. 54 ust. 1.

Artykuł 45

Incydenty bezpieczeństwa

1. Każde zdarzenie, które ma lub może mieć wpływ na bezpieczeństwo SIS lub może spowodować uszkodzenie lub utratę danych SIS lub informacji uzupełniających, uznaje się za incydent bezpieczeństwa, w szczególności jeżeli mogło dojść do uzyskania niezgodnego z prawem dostępu do danych lub jeżeli zostały lub mogły zostać naruszone dostępność, integralność i poufność danych.

2. Incydentami bezpieczeństwa zarządza się w sposób zapewniający szybkie, skuteczne i właściwe reagowanie.

3. Bez uszczerbku dla zgłaszania naruszenia ochrony danych osobowych i zawiadamiania o takim naruszeniu zgodnie z art. 33 rozporządzenia (UE) 2016/679 lub art. 30 dyrektywy (UE) 2016/680, państwa członkowskie, Europol oraz Europejska Agencja Straży Granicznej i Przybrzeżnej niezwłocznie powiadamiają Komisję, eu-LISA, właściwy organ nadzorczy i Europejskiego Inspektora Ochrony Danych o incydentach bezpieczeństwa. eu-LISA niezwłocznie powiadamia Komisję i Europejskiego Inspektora Ochrony Danych o każdym incydencie bezpieczeństwa dotyczącym systemu centralnego SIS.

4. Informacje o incydencie bezpieczeństwa, który ma lub może mieć wpływ na funkcjonowanie SIS w państwie członkowskim lub w eu-LISA, który ma lub może mieć wpływ na dostępność, integralność i poufność danych wprowadzonych lub przesłanych przez inne państwa członkowskie lub na informacje uzupełniające podlegające wymianie, są niezwłocznie przekazywane wszystkim państwom członkowskim i zgłaszane zgodnie z opracowanym przez eu-LISA planem zarządzania na wypadek incydentów bezpieczeństwa.

5. Państwa członkowskie i eu-LISA współpracują ze sobą w przypadku wystąpienia incydentu bezpieczeństwa.

6. Komisja natychmiast informuje o poważnych incydentach Parlament Europejski i Radę. Informacje takie opatrywane są klauzulą EU RESTRICTED/RESTREINT UE, zgodnie z mającymi zastosowanie przepisami bezpieczeństwa.

7. Jeżeli incydent bezpieczeństwa jest spowodowany wykorzystaniem danych niezgodnie z przeznaczeniem, państwa członkowskie, Europol oraz Europejska Agencja Straży Granicznej i Przybrzeżnej zapewniają zastosowanie sankcji zgodnie z art. 59.

Artykuł 46

Rozróżnianie osób o podobnych cechach

1. W przypadku stwierdzenia przy wprowadzaniu nowego wpisu, że w SIS istnieje już wpis dotyczący osoby z takim samym opisem tożsamości, biuro SIRENE w terminie 12 godzin zwraca się w drodze wymiany informacji uzupełniających do państwa członkowskiego dokonującego wpisu o wyjaśnienie, czy oba wpisy dotyczą tej samej osoby.

2. Jeżeli w wyniku sprawdzania okaże się, że osoba, której dotyczy nowy wpis, oraz osoba, której dotyczy wpis wprowadzony wcześniej do SIS, to rzeczywiście ta sama osoba, biuro SIRENE stosuje procedurę wprowadzania wielokrotnych wpisów, o której mowa w art. 23.

3. Jeżeli w wyniku sprawdzenia okaże się, że chodzi faktycznie o dwie różne osoby, biuro SIRENE zatwierdza wniosek o wprowadzenie drugiego wpisu, dodając dane niezbędne do zapobieżenia błędnej identyfikacji.

Artykuł 47

Dane dodatkowe wprowadzane w celu rozwiązywania problemów związanych z przywłaszczaniem tożsamości

1. Jeżeli istnieje ryzyko pomylenia osoby, której ma dotyczyć wpis, z osobą, której tożsamość została przywłaszczona, państwo członkowskie dokonujące wpisu uzupełnia wpis, za wyraźną zgodą osoby, której tożsamość została przywłaszczona, o dotyczące jej dane w celu zapobieżenia negatywnym skutkom błędnej identyfikacji. Osoba, której tożsamość została przywłaszczona, ma prawo do wycofania swojej zgody na przetwarzanie takich dodanych danych osobowych.

2. Dane osoby, której tożsamość została przywłaszczona, wykorzystywane są wyłącznie w celach:

a) umożliwienia właściwemu organowi odróżnienia osoby, której tożsamość została przywłaszczona, od osoby, której faktycznie ma dotyczyć wpis; oraz

b) umożliwienia osobie, której tożsamość została przywłaszczona, udowodnienia swojej tożsamości i wykazania, że jej tożsamość została przywłaszczona.

3. Na użytek niniejszego artykułu i pod warunkiem uzyskania wyraźnej zgody osoby, której tożsamość została przywłaszczona, w odniesieniu do każdej kategorii danych, wprowadzane do SIS i dalej w nim przetwarzane mogą być wyłącznie następujące dane osobowe osoby, której tożsamość została przywłaszczona:

a) nazwiska;

b) imiona;

c) imiona i nazwiska nadane przy urodzeniu;

d) poprzednio używane imiona i nazwiska oraz pseudonimy, w miarę możliwości wpisane oddzielnie;

e) szczególne obiektywne cechy fizyczne niepodlegające zmianom;

f) miejsce urodzenia;

g) data urodzenia;

h) płeć;

i) fotografie i wizerunki twarzy;

j) odbitki linii papilarnych palców, odbitki linii papilarnych dłoni lub odbitki linii papilarnych palców oraz dłoni;

k) wszelkie posiadane obywatelstwa;

l) kategoria dokumentów identyfikacyjnych danej osoby;

m) państwo wydania dokumentów identyfikacyjnych danej osoby;

n) numer lub numery dokumentów identyfikacyjnych danej osoby;

o) data wydania dokumentów identyfikacyjnych danej osoby;

p) adres danej osoby;

q) imię i nazwisko ojca danej osoby;

r) imię i nazwisko matki danej osoby.

4. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów technicznych niezbędnych do wprowadzania i dalszego przetwarzania danych, o których mowa w ust. 3 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

5. Dane, o których mowa w ust. 3, są usuwane w tym samym czasie, co odpowiadający im wpis, lub wcześniej, jeśli dana osoba o to wystąpi.

6. Dostęp do danych, o których mowa w ust. 3, mogą uzyskać wyłącznie organy mające prawo do dostępu do wpisu odpowiadającego tym danym. Mogą one z niego korzystać wyłącznie w celu zapobieżenia błędnej identyfikacji.

Artykuł 48

Odsyłacze pomiędzy wpisami

1. Państwo członkowskie może utworzyć odsyłacz pomiędzy wpisami, które wprowadza do SIS. Celem utworzenia takiego odsyłacza jest ustanowienie związku między dwoma wpisami lub większą liczbą wpisów.

2. Utworzenie odsyłacza nie wpływa na konkretne działanie, które ma zostać podjęte na podstawie każdego z tak powiązanych wpisów, ani na termin weryfikacji każdego z tak powiązanych wpisów.

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

4. Państwo członkowskie tworzy odsyłacz pomiędzy wpisami, jeżeli jest to uzasadnione potrzebą operacyjną.

5. Jeżeli państwo członkowskie uzna, że utworzenie przez inne państwo członkowskie odsyłacza pomiędzy wpisami 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 tego odsyłacza swoim organom znajdującym się poza jego terytorium.

6. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów technicznych dotyczących tworzenia odsyłaczy między wpisami. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

Artykuł 49

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, które biuro SIRENE przechowuje w plikach w wyniku wymiany informacji, utrzymywane są wyłącznie przez okres wymagany do osiągnięcia celów, w których zostały dostarczone. Są one usuwane najpóźniej po upływie jednego roku od daty usunięcia z SIS związanego z nimi wpisu.

3. Ust. 2 pozostaje bez uszczerbku dla prawa państwa członkowskiego do utrzymywania w plikach krajowych danych dotyczących konkretnego wpisu, który został wprowadzony przez to państwo członkowskie, lub wpisu, w związku z którym podjęto działanie na jego terytorium. Okres przechowywania takich danych w takich plikach reguluje prawo krajowe.

Artykuł 50

Przekazywanie danych osobowych stronom trzecim

Dane przetwarzane w SIS oraz powiązane informacje uzupełniające podlegające wymianie na mocy niniejszego rozporządzenia nie są przekazywane ani udostępniane państwom trzecim ani organizacjom międzynarodowym.

ROZDZIAŁ IX

OCHRONA DANYCH

Artykuł 51

Mające zastosowanie przepisy

1. Rozporządzenie (UE) 2018/1725 ma zastosowanie do przetwarzania danych osobowych przez eu-LISA i Europejską Agencję Straży Granicznej i Przybrzeżnej na mocy niniejszego rozporządzenia. Do przetwarzania danych osobowych przez Europol na mocy niniejszego rozporządzenia zastosowanie ma rozporządzenie (UE) 2016/794.

2. Do przetwarzania danych osobowych na mocy niniejszego rozporządzenia przez właściwe organy, o których mowa w art. 34 niniejszego rozporządzenia, zastosowanie ma rozporządzenie (UE) 2016/679, z wyjątkiem przetwarzania do celów zapobiegania przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych lub ich ścigania lub wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, w którym to przypadku zastosowanie ma dyrektywa (UE) 2016/680.

Artykuł 52

Prawo do informacji

1. Obywatele państwa trzeciego, których dotyczy wpis w SIS, są informowani o tym zgodnie z art. 13 i 14 rozporządzenia (UE) 2016/679 lub art. 12 i 13 dyrektywy (UE) 2016/680. Informacje te są przekazywane na piśmie wraz z kopią decyzji krajowej, o której mowa w art. 24 ust. 1 niniejszego rozporządzenia i która jest podstawą wpisu, lub wraz z odniesieniem do takiej decyzji.

2. Informacje te nie są przekazywane, jeżeli prawo krajowe pozwala ograniczyć prawo do informacji, w szczególności ze względu na ochronę bezpieczeństwa narodowego, obronność, bezpieczeństwo publiczne oraz w celu zapobiegania przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych i ich ścigania.

Artykuł 53

Prawo do dostępu, sprostowania nieprawidłowych danych i usuwania danych przechowywanych niezgodnie z prawem

1. Osoby, których dane dotyczą, mogą korzystać z praw przewidzianych w art. 15, 16 i 17 rozporządzenia (UE) 2016/679 oraz w art. 14 i art. 16 ust. 1 i 2 dyrektywy (UE) 2016/680.

2. Państwo członkowskie, inne niż państwo członkowskie dokonujące wpisu, może przekazać osobie, której dane dotyczą, informację o danych stanowiących jej dane osobowe, które są przetwarzane, wyłącznie w sytuacji, gdy najpierw umożliwiło państwu członkowskiemu dokonującemu wpisu zajęcie w tej sprawie stanowiska. Komunikacja pomiędzy państwami członkowskimi odbywa się w takich przypadkach w drodze wymiany informacji uzupełniających.

3. Państwo członkowskie podejmuje decyzję o nieprzekazywaniu całości lub części informacji osobie, której dane dotyczą, zgodnie z prawem krajowym, w zakresie – a także przez tak długi okres – w jakim takie częściowe lub całkowite ograniczenie stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym, przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów osoby, której dane dotyczą, po to aby:

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

b) uniemożliwić utrudnianie zapobiegania przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych lub ich ścigania lub wykonywania kar;

c) chronić bezpieczeństwo publiczne;

d) chronić bezpieczeństwo narodowe; lub

e) chronić prawa i wolności innych osób.

W przypadkach, o których mowa w akapicie pierwszym, państwo członkowskie bez zbędnej zwłoki informuje na piśmie osobę, której dane dotyczą, o odmowie lub ograniczeniu dostępu oraz o powodach takiej odmowy lub takiego ograniczenia. Informacje takie można pominąć, jeżeli ich przekazanie godziłoby w którykolwiek z celów określonych w akapicie pierwszym lit. a)–e). Państwo członkowskie informuje osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub możliwości skorzystania ze środka ochrony prawnej przed sądem.

Państwo członkowskie dokumentuje faktyczne lub prawne powody swojej decyzji o nieinformowaniu osoby, której dane dotyczą. Informacje te udostępnia się organom nadzorczym.

W takich przypadkach osoba, której dane dotyczą, może również wykonywać swoje prawa za pośrednictwem właściwych organów nadzorczych.

4. Po złożeniu wniosku o dostęp, sprostowanie lub usunięcie osoba, której dane dotyczą, jest informowana przez państwo członkowskie jak najszybciej, a w każdym razie nie później niż w terminach, o których mowa w art. 12 ust. 3 rozporządzenia (UE) 2016/679, o działaniach podjętych w związku ze skorzystaniem przez nią z tych praw na mocy niniejszego artykułu, niezależnie od tego, czy osoba, której te dane dotyczą, przebywa w państwie trzecim.

Artykuł 54

Środki ochrony prawnej

1. Bez uszczerbku dla przepisów dotyczących środków ochrony prawnej zawartych w rozporządzeniu (UE) 2016/679 i dyrektywie (UE) 2016/680 każdej osobie przysługuje prawo do wniesienia do właściwego organu, w tym sądu, na mocy prawa krajowego państwa członkowskiego żądania o dostęp do informacji, ich sprostowanie, ich usunięcie lub ich uzyskanie lub o zapłatę odszkodowania w związku z wpisem dotyczącym tej osoby.

2. Państwa członkowskie zobowiązują się wzajemnie do wykonywania orzeczeń lub decyzji kończących postępowanie w sprawie wydanych przez sądy lub organy, o których mowa w ust. 1 niniejszego artykułu, bez uszczerbku dla art. 58.

3. Państwa członkowskie raz w roku składają Europejskiej Radzie Ochrony Danych sprawozdanie na temat:

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

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

c) liczby wniosków o sprostowanie nieprawidłowych danych oraz o usunięcie danych przechowywanych niezgodnie z prawem przekazanych administratorowi danych oraz liczby przypadków, w których dane zostały sprostowane lub usunięte;

d) liczby przekazanych organowi nadzorczemu wniosków o sprostowanie nieprawidłowych danych oraz o usunięcie danych przechowywanych niezgodnie z prawem;

e) liczby wszczętych postępowań sądowych;

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

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

Komisja opracuje szablon sprawozdania, o którym mowa w niniejszym ustępie.

4. Sprawozdania państw członkowskich są włączane do wspólnego sprawozdania, o którym mowa w art. 57 ust. 4.

Artykuł 55

Nadzór nad N.SIS

1. Państwa członkowskie zapewniają, by niezależne organy nadzorcze wyznaczone w każdym państwie członkowskim, którym to organom powierzono uprawnienia określone w rozdziale VI rozporządzenia (UE) 2016/679 lub w rozdziale VI dyrektywy (UE) 2016/680, monitorowały zgodność z prawem przetwarzania danych osobowych w SIS na ich terytorium, przekazywania tych danych z ich terytorium oraz wymiany i dalszego przetwarzania informacji uzupełniających na ich terytorium.

2. Organy nadzorcze zapewniają, by co najmniej co cztery lata przeprowadzany był audyt operacji przetwarzania danych w ramach ich N.SIS zgodnie z międzynarodowymi standardami audytu. Audyt jest prowadzony przez organy nadzorcze albo organy nadzorcze bezpośrednio zlecają przeprowadzenie audytu niezależnemu audytorowi ds. ochrony danych. Organy nadzorcze zawsze zachowują kontrolę nad niezależnym audytorem i pełnią obowiązki niezależnego audytora.

3. Państwa członkowskie zapewniają, by organy nadzorcze dysponowały zasobami wystarczającymi do wykonywania zadań powierzonych im na mocy niniejszego rozporządzenia oraz miały dostęp do doradztwa świadczonego przez osoby posiadające wystarczającą wiedzę w zakresie danych biometrycznych.

Artykuł 56

Nadzór nad eu-LISA

1. Europejski Inspektor Ochrony Danych odpowiada za monitorowanie przetwarzania danych osobowych przez eu-LISA oraz za zapewnienie, by było ono prowadzone zgodnie z niniejszym rozporządzeniem. Zastosowanie mają odpowiednio zadania i uprawnienia, o których mowa w art. 57 i 58 rozporządzenia (UE) 2018/1725.

2. Europejski Inspektor Ochrony Danych co najmniej co cztery lata przeprowadza audyt w zakresie przetwarzania danych osobowych przez eu-LISA zgodny z międzynarodowymi standardami audytu. Sprawozdanie z tego audytu przesyłane jest Parlamentowi Europejskiemu, Radzie, eu-LISA, Komisji i organom nadzorczym. eu-LISA umożliwia się przedstawienie uwag przed przyjęciem sprawozdania.

Artykuł 57

Współpraca organów nadzorczych i Europejskiego Inspektora Ochrony Danych

1. Organy nadzorcze i Europejski Inspektor Ochrony Danych, działając w ramach swoich odpowiednich kompetencji, współpracują aktywnie w zakresie swoich zadań i zapewniają skoordynowany nadzór nad SIS.

2. Organy nadzorcze i Europejski Inspektor Ochrony Danych w zależności od potrzeb i w ramach swoich kompetencji przeprowadzają wymianę stosownych informacji, wspomagają się wzajemnie w przeprowadzaniu audytów i inspekcji, analizują trudności w zakresie wykładni lub stosowania niniejszego rozporządzenia i innych mających zastosowanie aktów prawnych Unii, badają problemy, które wykryto w wyniku sprawowania niezależnego nadzoru lub wykonywania praw przez osoby, których dane dotyczą, sporządzają uzgodnione propozycje wspólnych rozwiązań problemów oraz upowszechniają wiedzę o prawach w zakresie ochrony danych.

3. W celach określonych w ust. 2 organy nadzorcze i Europejski Inspektor Ochrony Danych spotykają się co najmniej dwa razy w roku w ramach Europejskiej Rady Ochrony Danych. Za koszty i obsługę tych posiedzeń odpowiada Europejska Rada Ochrony Danych. Podczas pierwszego posiedzenia zostanie przyjęty regulamin wewnętrzny. Dalsze metody pracy opracowuje się wspólnie stosownie do potrzeb.

4. Wspólne sprawozdanie z działalności dotyczącej skoordynowanego nadzoru przesyłane jest co roku przez Europejską Radę Ochrony Danych Parlamentowi Europejskiemu, Radzie i Komisji.

ROZDZIAŁ X

ODPOWIEDZIALNOŚĆ I SANKCJE

Artykuł 58

Odpowiedzialność

1. Bez uszczerbku dla prawa do odszkodowania oraz odpowiedzialności na mocy rozporządzenia (UE) 2016/679, dyrektywy (UE) 2016/680 i rozporządzenia (UE) 2018/1725:

a) osoba lub państwo członkowskie, które poniosły szkodę majątkową lub niemajątkową w wyniku niezgodnej z prawem operacji przetwarzania danych osobowych w związku z użytkowaniem N.SIS lub innego działania niezgodnego z niniejszym rozporządzeniem przeprowadzonych przez jedno z państw członkowskich, są uprawnione do odszkodowania od tego państwa członkowskiego; oraz

b) osoba lub państwo członkowskie, które poniosły szkodę majątkową lub niemajątkową w wyniku działania eu-LISA niezgodnego z niniejszym rozporządzeniem, są uprawnione do otrzymania odszkodowania od eu-LISA.

Państwo członkowskie lub eu-LISA zostają zwolnione z odpowiedzialności na podstawie akapitu pierwszego, w całości lub w części, jeżeli wykażą, że nie ponoszą odpowiedzialności za zdarzenie, które spowodowało szkodę.

2. Jeżeli niewypełnienie przez państwo członkowskie obowiązków spoczywających na nim zgodnie z niniejszym rozporządzeniem spowoduje szkodę w SIS, wówczas to państwo członkowskie ponosi odpowiedzialność za tę szkodę, chyba że – i w zakresie w jakim – eu-LISA lub inne państwo członkowskie uczestniczące w SIS nie podjęły rozsądnych środków, by zapobiec wystąpieniu szkody lub zminimalizować jej skutki.

3. Kwestie związane z roszczeniami o odszkodowanie wnoszonymi przeciwko państwu członkowskiemu z tytułu szkody, o której mowa w ust. 1 i 2, regulują przepisy prawa krajowego tego państwa członkowskiego. Roszczenia o odszkodowanie wnoszone przeciwko eu-LISA z tytułu szkody, o której mowa w ust. 1 i 2, podlegają warunkom przewidzianym w Traktatach.

Artykuł 59

Sankcje

Państwa członkowskie zapewniają, aby wszelkie przypadki niezgodnego z niniejszym rozporządzeniem wykorzystania danych SIS, przetwarzania takich danych lub wymiany informacji uzupełniających podlegały sankcjom zgodnie z prawem krajowym.

Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające.

ROZDZIAŁ XI

PRZEPISY KOŃCOWE

Artykuł 60

Monitorowanie i statystyki

1. eu-LISA zapewnia, by istniały procedury pozwalające monitorować, czy SIS działa zgodnie z wyznaczonymi celami, w tym w odniesieniu do wyników, opłacalności, bezpieczeństwa i jakości usług.

2. Na użytek prac konserwacyjno-technicznych, przygotowywania sprawozdań, sprawozdawczości na temat jakości danych i sporządzania statystyk eu-LISA ma dostęp do niezbędnych informacji związanych z operacjami przetwarzania danych wykonywanymi w systemie centralnym SIS.

3. eu-LISA sporządza dzienne, miesięczne i roczne statystyki pokazujące liczbę rekordów przypadających na daną kategorię wpisów, zarówno w odniesieniu do poszczególnych państw członkowskich, jak i w ujęciu zagregowanym. eu-LISA sporządza również roczne sprawozdania na temat liczby uzyskanych w systemie trafień przypadających na daną kategorię wpisów, liczby wyszukiwań w SIS oraz liczby przypadków skorzystania z dostępu do SIS w celu wprowadzenia, zaktualizowania lub usunięcia wpisu, zarówno w odniesieniu do poszczególnych państw członkowskich, jak i w ujęciu zagregowanym. Takie statystyki zawierają dane dotyczące wymiany informacji na podstawie art. 27–31. Sporządzane statystyki nie zawierają żadnych danych osobowych. Roczne sprawozdanie statystyczne podlega publikacji.

4. Państwa członkowskie, Europol i Europejska Agencja Straży Granicznej i Przybrzeżnej przekazują eu-LISA i Komisji informacje niezbędne do sporządzenia sprawozdań, o których mowa w ust. 3, 5, 7 i 8.

5. eu-LISA przekazuje Parlamentowi Europejskiemu, Radzie, państwom członkowskim, Komisji, Europolowi, Europejskiej Agencji Straży Granicznej i Przybrzeżnej oraz Europejskiemu Inspektorowi Ochrony Danych sporządzone przez siebie sprawozdania statystyczne.

Aby móc monitorować wdrażanie unijnych aktów prawnych, w tym do celów rozporządzenia (UE) nr 1053/2013, Komisja może zwrócić się do eu-LISA o regularne lub doraźne sporządzanie dodatkowych szczególnych sprawozdań statystycznych dotyczących działania SIS, użytkowania SIS i wymiany informacji uzupełniających.

Europejska Agencja Straży Granicznej i Przybrzeżnej może zwrócić się do eu-LISA o regularne lub doraźne sporządzanie dodatkowych szczególnych sprawozdań statystycznych do celów przeprowadzania analiz ryzyka i ocen narażenia, o których mowa w art. 11 i 13 rozporządzenia (UE) 2016/1624.

6. Na użytek art. 15 ust. 4 oraz ust. 3, 4 i 5 niniejszego artykułu eu-LISA ustanawia, wdraża i obsługuje w swoich centrach technicznych centralne repozytorium zawierające dane, o których mowa w art. 15 ust. 4 oraz w ust. 3 niniejszego artykułu, które nie umożliwią identyfikacji poszczególnych osób, ale umożliwią Komisji oraz agencjom wymienionym w ust. 5 niniejszego artykułu uzyskanie dostosowanych do ich potrzeb sprawozdań i statystyk. Na wniosek eu-LISA udziela państwom członkowskim, Komisji, Europolowi i Europejskiej Agencji Straży Granicznej i Przybrzeżnej – w zakresie, w jakim jest to niezbędne do wykonywania ich zadań – dostępu do centralnego repozytorium poprzez bezpieczny dostęp za pośrednictwem infrastruktury łączności. eu-LISA wprowadza kontrole dostępu i specjalne profile użytkownika, aby zapewnić, by dostęp do centralnego repozytorium był wykorzystywany wyłącznie do celu sporządzania sprawozdań i statystyk.

7. Dwa lata po dacie rozpoczęcia stosowania niniejszego rozporządzenia zgodnie z art. 66 ust. 5 akapit pierwszy, a następnie co dwa lata eu-LISA przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie na temat technicznych aspektów funkcjonowania systemu centralnego SIS i infrastruktury łączności, w tym kwestii ich bezpieczeństwa, Automatycznego Systemu Identyfikacji Daktyloskopijnej oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi. Sprawozdanie to zawiera również ocenę wykorzystywania wizerunków twarzy do identyfikowania osób, po tym jak technologia ta zostanie wprowadzona do użytku.

8. Trzy lata po dacie rozpoczęcia stosowania niniejszego rozporządzenia zgodnie z art. 66 ust. 5 akapit pierwszy, a następnie co cztery lata Komisja przeprowadza ogólną ocenę systemu centralnego SIS oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi. W tej ogólnej ocenie zawiera się analizę osiągniętych wyników w zestawieniu z celami i ocenia się, na ile wciąż aktualne są pierwotne przesłanki, w jaki sposób niniejsze rozporządzenie stosowane jest do systemu centralnego SIS, na ile bezpieczny jest system centralny SIS i jakie będą konsekwencje dla przyszłych operacji. Sprawozdanie z oceny zawiera także ocenę Automatycznego Systemu Identyfikacji Daktyloskopijnej oraz kampanii informacyjnych na temat SIS przeprowadzonych przez Komisję zgodnie z art. 19.

Sprawozdanie z oceny zawiera również statystyki dotyczące liczby wpisów wprowadzonych zgodnie z art. 24 ust. 1 lit. a) oraz statystyki dotyczące liczby wpisów wprowadzonych zgodnie z lit. b) tego ustępu. W odniesieniu do wpisów, które objęte są zakresem art. 24 ust. 1 lit. a), określa ono liczbę wpisów dokonanych w wyniku sytuacji, o których mowa w art. 24 ust. 2 lit. a) b) lub c). Sprawozdanie z oceny zawiera również ocenę stosowania art. 24 przez państwa członkowskie.

Komisja przekazuje sprawozdanie z oceny Parlamentowi Europejskiemu i Radzie.

9. Komisja przyjmuje akty wykonawcze w celu określenia szczegółowych zasad dotyczących funkcjonowania centralnego repozytorium, o którym mowa w ust. 6 niniejszego artykułu, oraz zasad ochrony danych i zasad bezpieczeństwa mających zastosowanie do tego repozytorium. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 62 ust. 2.

Artykuł 61

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 33 ust. 4, powierza się Komisji na czas nieokreślony od dnia 27 grudnia 2018 r.

3. Przekazanie uprawnień, o którym mowa w art. 33 ust. 4, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 33 ust. 4 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 62

Procedura komitetowa

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

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

Artykuł 63

Zmiany rozporządzenia (WE) nr 1987/2006

W rozporządzeniu (WE) nr 1987/2006 wprowadza się następujące zmiany:

1) art. 6 otrzymuje brzmienie:

„*Artykuł 6*

Systemy krajowe

1. Każde państwo członkowskie odpowiada za utworzenie, funkcjonowanie, utrzymanie i dalsze rozwijanie swojego N.SIS II oraz za przyłączenie go do NI-SIS.

2. Każde państwo członkowskie odpowiada za zapewnienie użytkownikom końcowym niezakłóconej dostępności danych SIS II.";

2) art. 11 otrzymuje brzmienie:

„*Artykuł 11*

Poufność – państwa członkowskie

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

2. W przypadku gdy dane państwo członkowskie współpracuje z wykonawcami zewnętrznymi przy zadaniach związanych z SIS II, ściśle monitoruje ono działania wykonawcy, by zapewnić przestrzeganie wszelkich przepisów niniejszego rozporządzenia, w szczególności dotyczących bezpieczeństwa, poufności i ochrony danych.

3. Zarządzania operacyjnego N.SIS II lub kopiami technicznymi nie powierza się przedsiębiorstwom prywatnym ani organizacjom prywatnym.";

3) w art. 15 wprowadza się następujące zmiany:

a) dodaje się ustęp w brzmieniu:

„3a. Organ zarządzający opracowuje i utrzymuje mechanizm i procedury do celów przeprowadzania kontroli jakości danych w CS-SIS. Przekazuje on państwom członkowskim regularne sprawozdania na ten temat.

Organ zarządzający przekazuje Komisji regularne sprawozdania, w których uwzględnia napotkane problemy i państwa członkowskie, których problemy te dotyczą.

Komisja przekazuje Parlamentowi Europejskiemu i Radzie regularne sprawozdania na temat napotkanych problemów związanych z jakością danych.";

b) ust. 8 otrzymuje brzmienie:

„8. Zarządzanie operacyjne centralnym SIS II obejmuje wszystkie zadania niezbędne do tego, by centralny SIS II działał zgodnie z niniejszym rozporządzeniem przez 24 godziny na dobę, 7 dni w tygodniu – w szczególności prace konserwacyjne oraz udoskonalenia techniczne niezbędne do sprawnego działania systemu. Zadania te obejmują również koordynowanie działań w zakresie testowania, zarządzanie tymi działaniami i ich wspieranie w odniesieniu do centralnego SIS II i N.SIS II, zapewniające funkcjonowanie centralnego SIS II i N.SIS II zgodnie z wymogami zgodności pod względem technicznym określonymi w art. 9.";

4) w art. 17 dodaje się ustępy w brzmieniu:

„3. W przypadku gdy organ zarządzający współpracuje z wykonawcami zewnętrznymi przy zadaniach związanych z SIS II, organ ten ściśle monitoruje działania wykonawcy, by zapewnić przestrzeganie wszystkich przepisów niniejszego rozporządzenia, w szczególności dotyczących bezpieczeństwa, poufności i ochrony danych.

4. Zarządzania operacyjnego CS-SIS nie powierza się przedsiębiorstwom prywatnym ani organizacjom prywatnym.";

5) w art. 20 ust. 2 dodaje się literę w brzmieniu:

„ka) rodzaj przestępstwa;";

6) w art. 21 dodaje się akapit w brzmieniu:

„Jeżeli decyzja o odmowie wjazdu i pobytu, o której mowa w art. 24 ust. 2, związana jest w przestępstwem terrorystycznym, dany przypadek uznaje się za wystarczająco adekwatny, odpowiedni i ważny, by uzasadniać wpis w SIS II. Ze względu na bezpieczeństwo publiczne lub narodowe państwa członkowskie mogą wyjątkowo nie wprowadzać wpisu, jeśli istnieje prawdopodobieństwo, że utrudniłby on prowadzenie dochodzeń urzędowych lub sądowych, postępowań przygotowawczych lub innych postępowań.";

7) art. 22 otrzymuje brzmienie:

„*Artykuł 22*

Przepisy szczegółowe dotyczące wprowadzania, weryfikacji lub wyszukiwania przy użyciu fotografii i odbitek linii papilarnych palców

1. Fotografie i odbitki linii papilarnych palców wprowadza się wyłącznie po przeprowadzeniu specjalnej kontroli jakości służącej stwierdzeniu, czy spełniają one minimalne normy jakości danych. Specyfikacja tej specjalnej kontroli jakości jest określana zgodnie z procedurą, o której mowa w art. 51 ust. 2.

2. Jeżeli fotografie i odbitki linii papilarnych palców są dostępne we wpisie w SIS II, takie fotografie i odbitki linii papilarnych palców wykorzystuje się do potwierdzenia tożsamości osoby, która została zlokalizowana w wyniku wyszukiwania alfanumerycznego przeprowadzonego w SIS II.

3. Wyszukiwanie przy użyciu odbitek linii papilarnych palców może być przeprowadzone we wszystkich przypadkach w celu identyfikacji danej osoby. Jednakże jeżeli tożsamości danej osoby nie można ustalić w żaden inny sposób, w celu identyfikacji przeprowadza się wyszukiwanie przy użyciu odbitek linii papilarnych palców. W tym celu centralny SIS II posiada Automatyczny System Identyfikacji Daktyloskopijnej.

4. Odbitki linii papilarnych palców w SIS II związane z wpisami wprowadzonymi zgodnie z art. 24 i 26 można wyszukiwać również przy użyciu kompletnych lub niekompletnych zestawów odbitek linii papilarnych palców, które znaleziono na miejscu popełnienia poważnych przestępstw lub przestępstw terrorystycznych będących przedmiotem postępowania przygotowawczego i w przypadku których z dużym prawdopodobieństwem można stwierdzić, że te zestawy odbitek linii papilarnych palców należą do sprawcy danego przestępstwa, pod warunkiem że wyszukiwanie przeprowadzane jest równolegle w odpowiednich bazach danych państw członkowskich zawierających odbitki linii papilarnych palców.";

8) art. 26 otrzymuje brzmienie:

„*Artykuł 26*

Warunki wprowadzania wpisów dotyczących obywateli państw trzecich, którzy są objęci środkami ograniczającymi

1. Wpisy dotyczące obywateli państw trzecich, którzy są objęci środkiem ograniczającym mającym zapobiec wjazdowi na terytorium państw członkowskich lub przejazdowi przez to terytorium, podejmowanymi zgodnie z aktami prawnymi przyjętymi przez Radę, w tym środkami służącymi wykonaniu zakazu podróżowania wydanego przez Radę Bezpieczeństwa Organizacji Narodów Zjednoczonych, są wprowadzane do SIS II na potrzeby odmowy wjazdu i pobytu, o ile spełnione są wymogi dotyczące jakości danych.

2. Wpisy wprowadza, aktualizuje i usuwa właściwy organ państwa członkowskiego, które w momencie przyjęcia danego środka sprawuje prezydencję w Radzie Unii Europejskiej. Jeżeli to państwo członkowskie nie ma dostępu do SIS II lub wpisów wprowadzonych zgodnie z niniejszym rozporządzeniem, obowiązek ten przejmuje państwo członkowskie, które ma sprawować kolejną prezydencję i ma dostęp do SIS II, w tym dostęp do wpisów wprowadzonych zgodnie z niniejszym rozporządzeniem.

Państwa członkowskie ustanawiają niezbędne procedury wprowadzania, aktualizowania i usuwania takich wpisów.";

9) dodaje się następujące artykuły w brzmieniu:

„*Artykuł 27a*

Dostęp Europolu do danych w SIS II

1. Jeżeli jest to niezbędne do wykonywania jej mandatu, Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), ustanowiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/794 (*) ma prawo do dostępu do danych w SIS II. Europol może również przeprowadzać ich wyszukiwania oraz może dokonywać wymiany informacji uzupełniających i występować z wnioskami o dalsze informacje uzupełniające zgodnie z zasadami zawartymi w podręczniku SIRENE.

2. Jeżeli podczas wyszukiwania Europol stwierdzi istnienie wpisu w SIS II, informuje o tym – w drodze wymiany informacji uzupełniających przy użyciu infrastruktury łączności i zgodnie z zasadami zawartymi w podręczniku SIRENE – państwo członkowskie dokonujące wpisu. Dopóki Europol nie będzie w stanie korzystać z funkcji przewidzianych do wymiany informacji uzupełniających, w celu przekazywania informacji państwom członkowskim dokonującym wpisu wykorzystuje kanały określone w rozporządzeniu (UE) 2016/794.

3. Europol może przetwarzać informacje uzupełniające, które przekazały mu państwa członkowskie, do celów przeprowadzania porównań ze swoimi bazami danych i projektami analitycznymi, mających służyć wskazaniu powiązań lub innych odpowiednich związków, oraz do celów analiz strategicznych, tematycznych lub operacyjnych, o których mowa w art. 18 ust. 2 lit. a), b) i c) rozporządzenia (UE) 2016/794. Europol przetwarza informacje uzupełniające do celów niniejszego artykułu zgodnie z tym rozporządzeniem.

4. Wykorzystanie przez Europol informacji uzyskanych w wyniku wyszukiwania w SIS II lub w wyniku przetwarzania informacji uzupełniających wymaga zgody państwa członkowskiego dokonującego wpisu. Jeżeli to państwo członkowskie zezwoli na wykorzystanie takich informacji, posługiwanie się nimi przez Europol regulowane jest rozporządzeniem (UE) 2016/794. Europol przekazuje takie informacje państwom trzecim i podmiotom trzecim wyłącznie za zgodą państwa członkowskiego dokonującego wpisu i z pełnym poszanowaniem prawa Unii dotyczącego ochrony danych.

5. Europol:

a) bez uszczerbku dla ust. 4 i 6 nie podłącza części SIS II ani nie przekazuje danych, które są w nim zawarte i do których ma dostęp, do żadnego systemu gromadzenia i przetwarzania danych stosowanego przez Europol lub w Europolu, a także nie pobiera ani w inny sposób nie kopiuje żadnych części SIS II;

b) niezależnie od art. 31 ust. 1 rozporządzenia (UE) 2016/794 usuwa informacje uzupełniające zawierające dane osobowe najpóźniej rok po usunięciu związanego z nimi wpisu. Na zasadzie odstępstwa, jeżeli Europol posiada w swoich bazach danych lub projektach analitycznych informacje o sprawie, której dotyczą informacje uzupełniające, w celu wykonywania swoich zadań Europol może wyjątkowo w razie potrzeby nadal przechowywać te informacje uzupełniające. Europol informuje państwo członkowskie dokonujące wpisu i wykonujące państwo członkowskie o dalszym przechowywaniu takich informacji uzupełniających i przedstawia uzasadnienie takiego dalszego przechowywania;

c) ogranicza dostęp do danych w SIS II, w tym do informacji uzupełniających, tak by korzystali z niego tylko specjalnie uprawnieni pracownicy Europolu, którym dostęp do takich danych jest potrzebny do wykonywania ich zadań;

d) przyjmuje i stosuje środki służące zapewnieniu bezpieczeństwa, poufności i monitorowania własnej działalności zgodnie z art. 10, 11 i 13;

e) zapewnia, by pracownicy uprawnieni do przetwarzania danych SIS II przeszli odpowiednie szkolenie i zostali odpowiednio poinformowani zgodnie z art. 14; oraz

f) bez uszczerbku dla rozporządzenia (UE) 2016/794 zapewnia Europejskiemu Inspektorowi Ochrony Danych możliwość monitorowania i kontrolowania działań podejmowanych przez Europol w ramach wykonywania prawa do dostępu do danych w SIS II i ich wyszukiwania oraz w ramach wymiany i przetwarzania informacji uzupełniających.

6. Europol kopiuje dane z SIS II wyłącznie do celów technicznych, jeżeli takie kopiowanie jest niezbędne do przeprowadzenia bezpośredniego wyszukiwania przez należycie uprawnionych pracowników Europolu. Do takich kopii zastosowanie ma niniejsze rozporządzenie. Kopię techniczną wykorzystuje się wyłącznie do przechowywania danych SIS II w trakcie przeprowadzania ich wyszukiwania. Po przeprowadzeniu wyszukiwania danych dane te są usuwane. Takich przypadków wykorzystywania danych nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie danych SIS II. Europol nie kopiuje do innych systemów Europolu danych zawartych we wpisach ani danych dodatkowych wprowadzonych przez państwa członkowskie lub pochodzących z CS-SIS II.

7. Do celów weryfikacji zgodności przetwarzania danych z prawem, monitorowania własnej działalności oraz zapewniania należytego bezpieczeństwa i integralności danych Europol rejestruje zgodnie z przepisami art. 12 każdy dostęp do SIS II oraz każde wyszukiwanie w SIS II. Prowadzenia takiej rejestracji i dokumentacji nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie części SIS II.

8. Państwa członkowskie informują Europol w drodze wymiany informacji uzupełniających o każdym trafieniu odnoszącym się do wpisów dotyczących przestępstw terrorystycznych. Państwa członkowskie mogą w wyjątkowych okolicznościach nie przekazywać Europolowi takich informacji, jeżeli takie przekazanie mogłoby spowodować zagrożenie dla realizowanych czynności lub bezpieczeństwa osób lub byłoby sprzeczne z istotnymi interesami w zakresie bezpieczeństwa państwa członkowskiego dokonującego wpisu.

9. Ust. 8 stosuje się od daty, z którą Europol będzie w stanie otrzymywać informacje uzupełniające zgodnie z ust. 1.

Artykuł 27b

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

1. Zgodnie z art. 40 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/1624 (**) członkowie zespołów, o których mowa w art. 2 pkt 8 i 9 tego rozporządzenia, mają – w ramach swojego mandatu oraz pod warunkiem że są uprawnieni do przeprowadzania kontroli zgodnie z art. 27 ust. 1 niniejszego rozporządzenia i przeszli wymagane szkolenie zgodnie z art. 14 niniejszego rozporządzenia – prawo do dostępu do danych w SIS II oraz do wyszukiwania takich danych w zakresie, w jakim jest to niezbędne do wykonywania ich zadań i zgodnie z wymogami planu operacyjnego dla danej operacji. Pozostali członkowie zespołów nie są uprawnieni do dostępu do danych w SIS II.

2. Członkowie zespołów, o których mowa w ust. 1, wykonują prawo do dostępu do danych w SIS II oraz do wyszukiwania takich danych zgodnie z ust. 1, korzystając z interfejsu technicznego. Interfejs techniczny zostanie utworzony i będzie prowadzony przez Europejską Agencję Straży Granicznej i Przybrzeżnej i będzie umożliwiał bezpośrednie połączenie z centralnym SIS II.

3. Jeżeli w wyniku wyszukiwania członek zespołów, o których mowa w ust. 1 niniejszego artykułu, stwierdzi istnienie wpisu w SIS II, powiadamia się o tym fakcie państwo członkowskie dokonujące wpisu. Zgodnie z art. 40 rozporządzenia (UE) 2016/1624 członkowie zespołów podejmują działania w odpowiedzi na wpis w SIS II wyłącznie na polecenie i – co do zasady – w obecności funkcjonariuszy straży granicznej lub personelu realizującego zadania w dziedzinie powrotów z przyjmującego państwa członkowskiego, w którym działają. Przyjmujące państwo członkowskie może upoważnić członków zespołów do działania w jego imieniu.

4. Do celów weryfikacji zgodności przetwarzania danych z prawem, monitorowania własnej działalności oraz zapewniania należytego bezpieczeństwa i integralności danych Europejska Agencja Straży Granicznej i Przybrzeżnej rejestruje zgodnie z przepisami art. 12 każdy dostęp do SIS II oraz każde wyszukiwanie w SIS II.

5. Europejska Agencja Straży Granicznej i Przybrzeżnej przyjmuje i stosuje środki służące zapewnieniu bezpieczeństwa, poufności i monitorowania własnej działalności zgodnie z art. 10, 11 i 13 oraz zapewnia, by zespoły, o których mowa w ust. 1 niniejszego artykułu, stosowały te środki.

6. Przepisów niniejszego artykułu nie można interpretować jako mających wpływ na przepisy rozporządzenia (UE) 2016/1624 dotyczące ochrony danych i odpowiedzialności Europejskiej Agencji Straży Granicznej i Przybrzeżnej za nieuprawnione lub nieprawidłowe przetwarzanie danych.

7. Bez uszczerbku dla ust. 2 żadnych części SIS II nie podłącza się do systemu gromadzenia i przetwarzania danych stosowanego przez zespoły, o których mowa w ust. 1 lub przez Europejską Agencję Straży Granicznej i Przybrzeżnej, a danych w SIS II, do których dostęp mają te zespoły, nie przekazuje się do takiego systemu. Nie można pobierać ani kopiować żadnych części SIS II. Rejestrowania dostępu i wyszukiwania nie uznaje się za niezgodne z przepisami pobieranie lub kopiowanie danych SIS II.

8. Europejska Agencja Straży Granicznej i Przybrzeżnej umożliwia Europejskiemu Inspektorowi Ochrony Danych monitorowanie i kontrolowanie działań prowadzonych przez zespoły, o których mowa w niniejszym artykule, w ramach wykonywania ich prawa do dostępu do danych w SIS II i wyszukiwania takich danych. Pozostaje to bez uszczerbku dla dalszych przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 (***).

(*) 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 24.5.2016, s. 53).

(**) 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).

(***) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).".

Artykuł 64

Zmiana w konwencji wykonawczej do układu z Schengen

Uchyla się art. 25 konwencji wykonawczej do układu z Schengen.

Artykuł 65

Uchylenie

Z dniem rozpoczęcia stosowania niniejszego rozporządzenia, określonym w art. 66 ust. 5 akapit pierwszy, uchyla się rozporządzenie (WE) nr 1987/2006.

Odesłania do uchylonego rozporządzenia traktuje się jako odesłania do niniejszego rozporządzenia i odczytuje się zgodnie z tabelą korelacji w załączniku.

Artykuł 66

Wejście w życie, rozpoczęcie eksploatacji i rozpoczęcie stosowania

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

2. Nie później niż w dniu 28 grudnia 2021 r. Komisja przyjmie decyzję określającą datę rozpoczęcia eksploatacji SIS zgodnie z niniejszym rozporządzeniem, po zweryfikowaniu, czy spełnione są następujące warunki:

a) przyjęto akty wykonawcze niezbędne do stosowania niniejszego rozporządzenia;

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

c) eu-LISA powiadomiła Komisję o pomyślnym zakończeniu wszystkich działań w zakresie testowania w odniesieniu do CS-SIS i interakcji między CS-SIS i N.SIS.

3. Komisja będzie monitoruje proces stopniowego spełniania warunków określonych w ust. 2 oraz informuje Parlament Europejski i Radę o wynikach weryfikacji, o której mowa w tym ustępie.

4. Do dnia 28 grudnia 2019 r., a następnie co roku do czasu przyjęcia przez Komisję decyzji, o której mowa w ust. 2, Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie o stanie przygotowań do pełnego wdrożenia niniejszego rozporządzenia. Sprawozdanie zawiera także szczegółowe informacje o poniesionych kosztach oraz informacje dotyczące wszelkich rodzajów ryzyka, które mogą mieć wpływ na ogólne koszty.

5. Niniejsze rozporządzenie stosuje się od daty określonej zgodnie z ust. 2.

Na zasadzie odstępstwa od akapitu pierwszego:

a) art. 4 ust. 4, art. 5, art. 8 ust. 4, art. 9 ust. 1 i 5, art. 15 ust. 7, art. 19, art. 20 ust. 3 i 4, art. 32 ust. 4, art. 33 ust. 4, art. 47 ust. 4, art. 48 ust. 6, art. 60 ust. 6 i 9, art. 61, art. 62, art. 63 pkt 1–6 i pkt 8 oraz ust. 3 i 4 niniejszego artykułu stosuje się od daty wejścia w życie niniejszego rozporządzenia;

b) art. 63 pkt 9 stosuje się od dnia 28 grudnia 2019 r.;

c) art. 63 pkt 7 stosuje się od dnia 28 grudnia 2020 r.

6. Decyzję Komisji, o której mowa w ust. 2, publikuje się w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane w państwach członkowskich zgodnie z Traktatami.

Sporządzono w Brukseli dnia 28 listopada 2018 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
A. TAJANI	K. EDTSTADLER
Przewodniczący	*Przewodnicząca*

ZAŁĄCZNIK

TABELA KORELACJI

Rozporządzenie (WE) nr 1987/2006	Niniejsze rozporządzenie
art. 1	art. 1
art. 2	art. 2
art. 3	art. 3
art. 4	at. 4
art. 5	art. 5
art. 6	art. 6
art. 7	art. 7
art. 8	art. 8
art. 9	art. 9
art. 10	art. 10
art. 11	art. 11
art. 12	art. 12
art. 13	art. 13
art. 14	art. 14
art. 15	art. 15
art. 16	art. 16
art. 17	art. 17
art. 18	art. 18
art. 19	art. 19
art. 20	art. 20
art. 21	art. 21
art. 22	art. 32 i 33
art. 23	art. 22
—	art. 23
art. 24	art. 24
art. 25	art. 26
art. 26	art. 25
—	art. 27
—	art. 28
—	art. 29
—	art. 30
—	art. 31
art. 27	art. 34
art. 27a	art. 35
art. 27b	art. 36
—	art. 37
art. 28	art. 38
art. 29	art. 39
art. 30	art. 40
art. 31	art. 41

Rozporządzenie (WE) nr 1987/2006	Niniejsze rozporządzenie
art. 32	art. 42
art. 33	art. 43
art. 34	art. 44
—	art. 45
art. 35	art. 46
art. 36	art. 47
art. 37	art. 48
art. 38	art. 49
art. 39	art. 50
art. 40	—
—	art. 51
art. 41	art. 53
art. 42	art. 52
art. 43	art. 54
art. 44	art. 55
art. 45	art. 56
art. 46	art. 57
art. 47	—
art. 48	art. 58
art. 49	art. 59
art. 50	art. 60
—	art. 61
art. 51	art. 62
art. 52	—
—	art. 63
—	art. 64
art. 53	—
—	art. 65
art. 54	—
art. 55	art. 66