



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)

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Utworzenie i ogólny cel SIS II

1. Niniejszym utworzony zostaje system informacyjny Schengen drugiej generacji („SIS II”).

2. Zgodnie z niniejszym rozporządzeniem celem SIS II jest zapewnienie przy wykorzystaniu z informacji przekazywanych za pośrednictwem tego systemu, wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej, w tym utrzymywanie bezpieczeństwa publicznego oraz porządku publicznego oraz zagwarantowanie bezpieczeństwa na terytorium państw członkowskich, a także stosowanie postanowień tytułu IV części trzeciej Traktatu odnoszących się do przepływu osób na terytorium państw członkowskich.

Artykuł 2

Zakres zastosowania

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

2. Ponadto niniejsze rozporządzenie ustanawia przepisy dotyczące struktury technicznej SIS II, obowiązków państw członkowskich i organu zarządzającego, o którym mowa w art. 15, ogólnego przetwarzania danych, praw osób zainteresowanych oraz odpowiedzialności.

Artykuł 3

Definicje

Na użytek niniejszego rozporządzenia stosuje się następujące definicje:

- a) „wpis” oznacza zbiór danych wprowadzonych do SIS II, umożliwiających właściwym organom zidentyfikowanie osoby w związku z konkretnym planowanym działaniem;
- b) „informacje uzupełniające” oznaczają informacje, które nie są przechowywane w SIS II, ale są związane z wpisami do SIS II, i które są wymieniane w następujących okolicznościach:
 - (i) w celu umożliwienia państwom członkowskim wzajemnej konsultacji lub wzajemnego informowania się podczas dokonywania wpisu;
 - (ii) w celu umożliwienia podjęcia odpowiednich działań po uzyskaniu potwierdzenia w systemie;
 - (iii) w przypadku niemożności podjęcia wymaganego działania;

▼ B

- (iv) w przypadku rozwiązywania kwestii jakości danych SIS II;
 - (v) w przypadku rozwiązywania kwestii zgodności i priorytetu wpisów;
 - (vi) w przypadku rozwiązywania kwestii związanych z prawami dostępu;
- c) „dane dodatkowe” oznaczają dane związane z wpisami do SIS II, które są przechowywane w SIS II, i które są natychmiast dostępne dla właściwych organów, gdy w wyniku poszukiwań prowadzonych w systemie znaleziono w nim osobę, której dane w nim umieszczono;
- d) „obywatel państwa trzeciego” oznacza każdego obywatela, który nie jest:
- (i) obywatelem Unii Europejskiej w rozumieniu art. 17 ust. 1 Traktatu WE; ani
 - (ii) obywatelem państwa trzeciego, który na mocy porozumień pomiędzy Wspólnotą i jej państwami członkowskimi a tymi państwami trzecimi korzysta z prawa swobodnego przemieszczania się równoważnego z prawem obywateli Unii Europejskiej;
- e) „dane osobowe” oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoba, której dotyczą dane”); osoba możliwa do zidentyfikowania to osoba, która może zostać zidentyfikowana bezpośrednio lub pośrednio;
- f) „przetwarzanie danych osobowych” („przetwarzanie”) oznacza każdą operację lub ciąg operacji dokonywanych na danych osobowych, także metodami automatycznej obróbki danych, takimi jak gromadzenie, zapis, porządkowanie, przechowywanie, dostosowywanie lub przekształcanie, odzyskiwanie, przeglądanie, wykorzystywanie, ujawnianie przez przekazanie, rozpowszechnianie lub udostępnianie w inny sposób, zestawianie lub kompilowanie, blokowanie, usuwanie lub niszczenie.

*Artykuł 4***Struktura techniczna i sposoby korzystania z SIS II**

1. SIS II składa się z:
 - a) systemu centralnego („centralny SIS II”) składającego się z następujących elementów:
 - funkcji wsparcia technicznego („CS-SIS”) zawierającej bazę danych („baza danych SIS II”);
 - jednolitego interfejsu krajowego („NI-SIS”);

▼B

b) systemu krajowego („N. SIS II”) w każdym państwie członkowskim, składającego się z krajowych systemów danych, które łączą się z centralnym SIS II. N-SIS II może zawierać plik danych („kopia krajowa”) zawierający pełną lub częściową kopię bazy danych SIS II;

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

2. Dane w SIS II wpisuje się, aktualizuje, usuwa i wyszukuje za pośrednictwem poszczególnych systemów N. SIS II. Kopia krajowa jest dostępna w celu prowadzenia automatycznego wyszukiwania na terytorium każdego państwa członkowskiego, które korzysta z takiej kopii. Przeszukiwanie plików danych zawartych w N. SIS II innych państw członkowskich nie jest możliwe.

3. CS-SIS, wykonujący funkcje nadzorcze i administracyjne, mieści się w Strasburgu, we Francji, natomiast rezerwowo CS-SIS, zdolny do zapewnienia wszystkich funkcji głównego CS-SIS w przypadku jego awarii, mieści się w Sankt Johann im Pongau, w Austrii.

4. CS-SIS zapewnia usługi konieczne do wprowadzania i przetwarzania danych SIS II, w tym do prowadzenia wyszukiwań w bazie danych SIS II. CS-SIS zapewnia państwom członkowskim korzystającym z kopii krajowej:

a) aktualizację kopii krajowych w trybie bezpośrednim (*on-line*);

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

c) czynności związane z inicjalizacją i odtwarzaniem kopii krajowych.

*Artykuł 5***Koszty**

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

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

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

▼B**ROZDZIAŁ II**
OBOWIĄZKI PAŃSTW CZŁONKOWSKICH**▼M2***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.

▼B*Artykuł 7*
Urząd N. SIS II i biuro SIRENE

1. Każde państwo członkowskie wyznacza organ, który na szczeblu centralnym odpowiada za N. SIS II tego państwa („urząd N. SIS II”). Organ ten odpowiada za sprawne działanie i bezpieczeństwo N. SIS II, zapewnia właściwym organom dostęp do SIS II i stosuje odpowiednie środki, aby zapewnić przestrzeganie przepisów niniejszego rozporządzenia. Każde państwo członkowskie przekazuje swoje wpisy za pośrednictwem urzędu N. SIS II.
2. Każde państwo członkowskie wyznacza organ („biuro SIRENE”), który zapewnia wymianę wszelkich informacji uzupełniających, o której mowa w art. 8, zgodnie z wytycznymi zawartymi w podręczniku SIRENE.

Powyższe biura koordynują również weryfikację jakości informacji wprowadzanych do SIS II. Aby realizować te cele, biura SIRENE posiadają dostęp do danych przetwarzanych w SIS II.
3. Państwa członkowskie informują organ zarządzający o swoim krajowym urzędzie N. SIS II i biurze SIRENE. Organ zarządzający publikuje wykaz tych urzędów i biur wraz z wykazem, o którym mowa w art. 31 ust. 8.

Artykuł 8
Wymiana informacji uzupełniających

1. Informacje uzupełniające są wymieniane zgodnie z wytycznymi zawartymi w „podręczniku SIRENE” za pośrednictwem infrastruktury łączności. W przypadku gdy infrastruktura łączności jest niedostępna, państwa członkowskie mogą wykorzystywać inne odpowiednio zabezpieczone środki techniczne do wymiany informacji uzupełniających.
2. Informacje uzupełniające są wykorzystywane wyłącznie do celu, w jakim zostały przekazane.

▼B

3. Odpowiedź na wniosek państwa członkowskiego o informacje uzupełniające jest udzielana niezwłocznie.

4. Szczegółowe zasady wymiany informacji uzupełniających są przyjmowane zgodnie z procedurą, o której mowa w art. 51 ust. 2, w formie podręcznika SIRENE, bez uszczerbku dla przepisów aktu ustanawiającego organ zarządzający.

*Artykuł 9***Zgodność techniczna**

1. Aby zapewnić szybki i sprawny przesył danych, każde państwo członkowskie, tworząc własny N. SIS II, przestrzega protokołów i procedur technicznych ustalonych, by zapewnić kompatybilność N. SIS II z CS-SIS. Wspomniane protokoły i procedury techniczne ustalane są zgodnie z procedurą, o której mowa w art. 51 ust. 2, bez uszczerbku dla przepisów aktu ustanawiającego organ zarządzający.

2. Jeżeli państwo członkowskie korzysta z kopii krajowej, jest ono zobowiązane zapewnić, korzystając z usług CS-SIS, by dane przechowywane w kopii krajowej były dzięki automatycznym aktualizacjom, o których mowa w art. 4 ust. 4, identyczne i spójne względem danych w bazie SIS II oraz by przeszukiwanie kopii krajowej prowadziło do takich samych wyników, jak przeszukiwanie bazy danych SIS II.

*Artykuł 10***Bezpieczeństwo - państwa członkowskie**

1. W odniesieniu do N. SIS II każde państwo członkowskie podejmuje odpowiednie środki, obejmujące plan bezpieczeństwa, tak aby:

- a) zapewnić fizyczną ochronę danych, m.in. poprzez sporządzenie planów awaryjnych służących ochronie infrastruktury krytycznej;
- b) zapobiec dostępowi osób nieuprawnionych do infrastruktury przetwarzania danych, wykorzystywanej do przetwarzania danych osobowych (kontrola dostępu do infrastruktury);
- c) zapobiec nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);
- d) zapobiec nieuprawnionemu wprowadzaniu danych i nieuprawnionemu wglądowi do przechowywanych danych osobowych oraz ich zmienianiu i usuwaniu (kontrola przechowywania);

▼ B

- e) zapobiec wykorzystywaniu systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, korzystające ze sprzętu do przekazywania danych (kontrola użytkowników);
- f) zapewnić, by osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania danych miały dostęp wyłącznie do danych objętych posiadaniem przez siebie upoważnieniem, poprzez osobiste i niepowtarzalne identyfikatory użytkownika oraz poufny tryb dostępu (kontrola dostępu do danych);
- g) zapewnić, by wszystkie organy mające prawo do dostępu do SIS II 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 przeszukiwania, oraz by profile te były bezzwłocznie udostępniane krajowym organom nadzorczym, o których mowa w art. 44 ust. 1, na ich wniosek (profile personelu);
- h) zapewnić możliwość weryfikacji i stwierdzenia, jakim organom można przekazywać dane osobowe za pośrednictwem sprzętu do przekazywania danych (kontrola przekazywania danych);
- i) zapewnić następnie możliwość późniejszej weryfikacji i stwierdzenia, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania danych oraz kiedy, przez kogo i w jakim celu dane te zostały wprowadzone (kontrola wprowadzania danych);
- j) zapobiec nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas transferu danych osobowych lub podczas przemieszczania nośników danych, w szczególności poprzez zastosowanie odpowiednich technik szyfrowania (kontrola transportu);
- k) kontrolować skuteczność środków bezpieczeństwa, o których mowa w niniejszym ustępie i podejmować konieczne działania organizacyjne dotyczące kontroli wewnętrznej, w celu zapewnienia przestrzegania niniejszego rozporządzenia (autokontrola).

2. W odniesieniu do bezpieczeństwa wymiany informacji uzupełniających państwa członkowskie podejmują środki równoważne środkom, o których mowa w ust. 1.

▼ M2*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.

▼ M2

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.

▼ B*Artykuł 12***Prowadzenie rejestrów na szczeblu krajowym**

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

2. Państwa członkowskie korzystające z kopii krajowych zapewniają rejestrowanie wszystkich przypadków, w których uzyskano dostęp do danych SIS II lub dokonano wymiany tych danych, w celach określonych w ust. 1. Nie dotyczy to działań, o których mowa w art. 4 ust. 4.

3. Rejestry zawierają w szczególności historię wpisów, datę i godzinę przekazania danych, dane wykorzystane do wyszukiwania, odniesienie do danych przekazanych oraz nazwę właściwego organu i nazwisko osoby odpowiedzialnej za przetwarzanie danych.

4. Rejestry mogą być wykorzystywane wyłącznie do celów określonych w ust. 1 i 2 oraz są usuwane najwcześniej po upływie jednego roku, a najpóźniej po upływie trzech lat od daty ich sporządzenia. Rejestry obejmujące historię wpisów są usuwane po upływie okresu od jednego roku do trzech lat od daty usunięcia wpisów.

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

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

▼ B*Artykuł 13***Autokontrola**

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

*Artykuł 14***Szkolenie personelu**

Przed otrzymaniem upoważnienia do przetwarzania danych przechowywanych w SIS II posiadający prawo do dostępu do SIS II pracownicy organów zostają odpowiednio przeszkoleni w zakresie bezpieczeństwa danych i zasad ochrony danych oraz są pouczani o związanych z tym przestępstwach i sankcjach.

ROZDZIAŁ III

OBOWIĄZKI ORGANU ZARZĄDZAJĄCEGO*Artykuł 15***Zarządzanie operacyjne**

1. Po upływie okresu przejściowego za zarządzanie operacyjne centralnym SIS II odpowiedzialny jest organ zarządzający, finansowany z budżetu ogólnego Unii Europejskiej. Organ zarządzający zapewnia we współpracy z państwami członkowskimi, by w centralnym SIS II były zawsze wykorzystywane najlepsze dostępne rozwiązania techniczne, wybierane na podstawie analizy korzyści i kosztów.

▼ M1

2. Organ zarządzający jest odpowiedzialny za realizację wszystkich zadań związanych z infrastrukturą łączności, w szczególności za:

- a) nadzór;
- b) bezpieczeństwo;
- c) koordynację stosunków między państwami członkowskimi a dostawcą usług;
- d) zadania związane z wykonywaniem budżetu;
- e) nabywanie i odnawianie;
- f) kwestie dotyczące umów.

▼ M2

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

4. W okresie przejściowym, do czasu podjęcia obowiązków przez organ zarządzający, za zarządzanie operacyjne centralnym SIS II odpowiedzialna jest Komisja. Komisja może powierzyć to zadanie oraz

▼ B

realizację zadań związanych z wykonywaniem budżetu, zgodnie z rozporządzeniem Rady (WE, Euratom) nr 1605/2002 z dnia 25 czerwca 2002 r. w sprawie rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich⁽¹⁾, krajowym organom sektora publicznego, które znajdują się w dwóch różnych państwach.

5. Każdy z krajowych organów sektora publicznego, o których mowa w ust. 4, musi spełniać w szczególności następujące kryteria wyboru:

- a) musi wykazać długie doświadczenie w eksploatacji wielkoskalowego systemu informatycznego o funkcjach, o których mowa w art. 4 ust. 4;
- b) musi posiadać znaczną wiedzę fachową na temat wymagań związanych z obsługą i bezpieczeństwem systemu informatycznego o funkcjach porównywalnych z funkcjami, o których mowa w art. 4 ust. 4;
- c) musi dysponować wystarczającą liczbą doświadczonych pracowników posiadających kwalifikacje zawodowe i językowe odpowiednie do współpracy w międzynarodowym środowisku wymagane dla potrzeb SIS II;
- d) musi dysponować bezpieczną i opracowaną specjalnie dla jego potrzeb infrastrukturą, zdolną w szczególności wspierać wielkoskalowe systemy informatyczne i zapewniać ich ciągłe działanie;

oraz

- e) jego otoczenie administracyjne musi umożliwiać właściwe wywiązywanie się z zadań i unikanie konfliktów interesów.

6. Przed delegowaniem zadań, o których mowa w ust. 4, a po dokonaniu tego, w regularnych odstępach czasowych, Komisja informuje Parlament Europejski i Radę o warunkach, na jakich zadania te zostały delegowane, dokładnym zakresie tych zadań oraz organach, którym zadania te delegowano.

7. Jeżeli w okresie przejściowym Komisja deleguje swoje obowiązki zgodnie z ust. 4, zapewnia ona, by zostały przy tym w pełni zachowane ograniczenia wynikające z systemu instytucjonalnego określonego w Traktacie. Komisja zapewnia w szczególności, by delegowanie tych zadań nie wpłynęło niekorzystnie na jakikolwiek system skutecznej kontroli ustanowiony prawem wspólnotowym, sprawowanej przez Trybunał Sprawiedliwości, Trybunał Obrachunkowy lub też przez Europejskiego Inspektora Ochrony Danych.

▼ M2

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

⁽¹⁾ Dz.U. L 248 z 16.9.2002, str. 1.

▼ M2

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.

▼ B*Artykuł 16***Bezpieczeństwo**

1. Organ zarządzający w odniesieniu do centralnego SIS II, a Komisja w odniesieniu do infrastruktury łączności podejmują niezbędne środki, obejmujące plan bezpieczeństwa, aby:

- a) zapewnić fizyczną ochronę danych, w tym poprzez sporządzenie planów awaryjnych służących ochronie infrastruktury krytycznej;
- b) zapobiec dostępowi osób nieuprawnionych do infrastruktury przetwarzania danych, wykorzystywanej do przetwarzania danych osobowych (kontrola dostępu do infrastruktury);
- c) zapobiec nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);
- d) zapobiec nieuprawnionemu wprowadzaniu danych i nieuprawnionemu wglądowi do przechowywanych danych osobowych oraz ich zmienianiu i usuwaniu (kontrola przechowywania);
- e) zapobiec wykorzystywaniu systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, korzystające ze sprzętu do przekazywania danych (kontrola użytkowników);
- f) zapewnić, by osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania danych miały dostęp wyłącznie do danych objętych posiadaniem przez siebie upoważnieniem, za pomocą osobistych i niepowtarzalnych identyfikatorów użytkownika oraz poufnego trybu dostępu (kontrola dostępu do danych);
- g) stworzyć profile z opisem funkcji i zadań osób, które są uprawnione do dostępu do danych lub do infrastruktury przetwarzania danych, i udostępnić te profile bezzwłocznie Europejskiemu Inspektorowi Ochrony Danych, o którym mowa w art. 45, na jego wniosek (profile personelu);
- h) zapewnić możliwość weryfikacji i stwierdzenia, jakim organom można przekazywać dane osobowe za pośrednictwem sprzętu do przekazywania danych (kontrola przekazywania danych);

▼B

- i) zapewnić następnie możliwość weryfikacji i stwierdzenia, które dane osobowe zostały wprowadzone do zautomatyzowanych systemów przetwarzania danych oraz kiedy i przez kogo zostały one wprowadzone (kontrola wprowadzania danych);
 - j) zapobiec nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas transferów danych osobowych lub podczas przemieszczania nośników danych w szczególności poprzez zastosowanie odpowiednich technik szyfrowania (kontrola transportu);
 - k) kontrolować skuteczność środków bezpieczeństwa, o których mowa w niniejszym ustępie, i podejmować konieczne działania organizacyjne dotyczące kontroli wewnętrznej, tak by spełnić wymogi niniejszego rozporządzenia (autokontrola).
2. W odniesieniu do bezpieczeństwa wymiany informacji uzupełniających za pomocą infrastruktury łączności organ zarządzający podejmuje środki bezpieczeństwa równoważne środkom, o których mowa w ust. 1.

*Artykuł 17***Poufność - organ zarządzający**

1. Bez uszczerbku dla art. 17 regulaminu pracowniczego urzędników Wspólnot Europejskich, organ zarządzający stosuje odpowiednie zasady tajemnicy zawodowej lub inne równoważne wymogi poufności wobec wszystkich swoich pracowników, którzy muszą operować danymi SIS II, na zasadach porównywalnych z zasadami, o których mowa w art. 11 niniejszego rozporządzenia. Zobowiązanie to obowiązuje także po zakończeniu pełnienia urzędu lub ustaniu zatrudnienia lub po zakończeniu ich działalności.
2. W odniesieniu do poufności wymiany informacji uzupełniających za pomocą infrastruktury łączności organ zarządzający podejmuje środki zapewniające poufność równoważne środkom, o których mowa w ust. 1.

▼M2

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.

▼B*Artykuł 18***Prowadzenie rejestrów na szczeblu centralnym**

1. Organ zarządzający zapewnia rejestrowanie wszystkich przypadków, w których uzyskano dostęp do danych osobowych w CS-SIS lub dokonano wymiany takich danych, do celów, o których mowa w art. 12 ust. 1 i 2.

▼B

2. Rejestry zawierają w szczególności historię wpisów, datę i godzinę przekazania danych, dane wykorzystane do wyszukiwania, odniesienie do przekazanych danych oraz nazwę właściwego organu odpowiedzialnego za przetwarzanie danych.
3. Rejestry mogą być wykorzystywane wyłącznie do celu wskazanego w ust. 1 i są usuwane najwcześniej po upływie jednego roku, a najpóźniej po upływie trzech lat od daty ich sporządzenia. Rejestry obejmujące historię wpisów są usuwane po upływie okresu od jednego roku do trzech lat od daty usunięcia wpisów.
4. Rejestry mogą być przechowywane dłużej, jeśli są potrzebne dla celów procedur monitorowania, które już się rozpoczęły.
5. Właściwe organy odpowiedzialne za kontrolowanie, czy dane wyszukiwanie jest dopuszczalne, monitorowanie dopuszczalności przetwarzania danych, autokontrolę i zapewnianie należytego działania N. SIS II, integralności danych i bezpieczeństwa, muszą w granicach swoich uprawnień, na żądanie mieć dostęp do tych rejestrów, do celów wykonywania swoich zadań.

*Artykuł 19***Kampania informacyjna**

Komisja — we współpracy z krajowymi organami nadzorczymi i Europejskim Inspektorem Ochrony Danych — dopilnowuje, by uruchomieniu SIS II towarzyszyła kampania informacyjna, informująca społeczeństwo o celach, przechowywanych danych, organach mających do nich dostęp oraz prawach obywateli. Po utworzeniu organu zarządzającego regularnie powtarza on takie kampanie we współpracy z krajowymi organami nadzorczymi i Europejskim Inspektorem Ochrony Danych. Państwa członkowskie, we współpracy z własnymi krajowymi organami nadzorczymi, opracowują i wprowadzają w życie konieczne strategie działań służące ogólnemu informowaniu społeczeństwa o SIS II.

ROZDZIAŁ IV

WPISY DOTYCZĄCE OBYWATELI PAŃSTW TRZECICH DOKONANE DO CELÓW ODMOWY POZWOLENIA NA WJAZD I POBYT*Artykuł 20***Kategorie danych**

1. Bez uszczerbku dla art. 8 ust. 1 ani dla tych przepisów niniejszego rozporządzenia, które odnoszą się do przechowywania danych dodatkowych, SIS II zawiera wyłącznie te kategorie danych, dostarczanych przez każde z państw członkowskich, tak jak tego wymagają cele określone w art. 24.
2. Informacje o osobach, w odniesieniu do których dokonano wpisu, nie zawierają innych danych niż:

▼ B

- a) nazwisko (nazwiska) i imię (imiona), nazwisko (nazwiska) rodowe, poprzednio używane imiona/nazwiska oraz wszelkie pseudonimy, które mogą być wpisywane oddzielnie;
- b) wszelkie szczególne, obiektywne cechy fizyczne niepodlegające zmianom;
- c) miejsce i data urodzenia;
- d) płeć;
- e) fotografie;
- f) odciski palców;
- g) obywatelstwo (obywatelstwa);
- h) informacja, czy dana osoba jest uzbrojona, agresywna lub czy jest uciekinierem;
- i) powód wpisu;
- j) organ dokonujący wpisu;
- k) odesłanie do decyzji będącej powodem wpisu;

▼ M2

- ka) rodzaj przestępstwa;

▼ B

- l) działania, jakie należy podjąć;
- m) odsyłacz lub odsyłacze do innych wpisów dokonanych w SIS II zgodnie z art. 37.

3. Techniczne zasady wpisywania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 2, są ustalane zgodnie z procedurą, o której mowa w art. 51 ust. 2, bez uszczerbku dla przepisów aktu ustanawiającego organ zarządzający.

4. Techniczne zasady konieczne do przeszukiwania danych, o których mowa w ust. 3, są podobne do zasad wyszukiwania w CS-SIS oraz w kopiach krajowych i technicznych, o których mowa w at. 31 ust. 2.

*Artykuł 21***Proporcjonalność**

Państwo członkowskie przed dokonaniem wpisu decyduje, czy dany przypadek jest na tyle stosowny, odpowiedni i ważny, by uzasadnione było wprowadzenie tego wpisu do SIS II.

▼ M2

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

▼ M2

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.

*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 równoległe w odpowiednich bazach danych państw członkowskich zawierających odbitki linii papilarnych palców.

▼ B*Artykuł 23***Wymóg warunkujący dokonanie wpisu**

1. Wpisu nie wolno dokonywać, jeśli brak jest danych, o których mowa w art. 20 ust. 2 lit. a), d), k) i l).
2. Wprowadzane są również wszystkie pozostałe dane wymienione w art. 20 ust. 2, o ile są dostępne.

*Artykuł 24***Warunki dokonywania wpisów dotyczących odmowy pozwolenia na wjazd lub pobyt**

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

▼B

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

- a) obywatela państwa trzeciego, który został skazany w państwie członkowskim za przestępstwo zagrożone karą pozbawienia wolności powyżej jednego roku;
- b) obywatela państwa trzeciego, co do którego istnieją uzasadnione powody, by sądzić, że popełnił poważne przestępstwa, lub co do którego istnieją poważne przesłanki, by sądzić, że zamierza on takie przestępstwa popełnić na terytorium państwa członkowskiego.

3. Wpisu można również dokonać, jeżeli decyzja, o której mowa w ust. 1, jest uzasadniona tym, że obywatel państwa trzeciego został poddany środkom obejmującym deportację, odmowę pozwolenia na wjazd lub wydalenie, które nie zostały unieważnione ani zawieszono i w których zawarte są lub którym towarzyszą zakaz wjazdu lub, stosownie do sytuacji, zakaz pobytu, z uwagi na naruszenie krajowych przepisów dotyczących wjazdu lub pobytu obywateli państw trzecich.

4. Niniejszy artykuł nie ma zastosowania do osób, o których mowa w art. 26.

5. Komisja dokonuje przeglądu stosowania niniejszego artykułu w terminie trzech lat od daty określonej w art. 55 ust. 2. Na podstawie tego przeglądu, Komisja korzystając ze swojego prawa inicjatywy określonego w Traktacie, przedstawia konieczne wnioski w sprawie zmiany przepisów niniejszego artykułu, tak aby osiągnąć wyższy poziom harmonizacji kryteriów dokonywania wpisów.

Artykuł 25

Warunki dokonywania wpisów dotyczących obywateli państw trzecich, którzy mogą korzystać z prawa do swobodnego przepływu w obrębie Wspólnoty

1. Wpis dotyczący obywatela państwa trzeciego, któremu przysługuje prawo do swobodnego przepływu w obrębie Wspólnoty w rozumieniu dyrektywy 2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przepływu i pobytu na terytorium państw członkowskich⁽¹⁾, dokonywany jest na podstawie przepisów przyjętych w celu wprowadzenia w życie tej dyrektywy.

2. W przypadku, gdy system potwierdził istnienie wpisu dokonanego zgodnie z art. 24 i dotyczącego obywatela państwa trzeciego, któremu przysługuje prawo do swobodnego przepływu w obrębie Wspólnoty, państwo członkowskie wykonujące wpis natychmiast konsultuje się za pośrednictwem biura SIRENE i zgodnie ze wskazówkami podręcznika SIRENE z państwem członkowskim, które dokonało wpisu, po to by bezzwłocznie podjąć decyzję co do wymaganych działań.

⁽¹⁾ Dz.U. L 158 z 30.4.2004, str. 77.

▼ **M2***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.

▼ **B***Artykuł 27***Organy uprawnione do dostępu do wpisów**

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

- a) kontroli granicznej, zgodnie z rozporządzeniem (WE) nr 562/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. ustanawiającym wspólnotowy kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) ⁽¹⁾;
- b) innych kontroli policyjnych i celnych prowadzonych na terytorium danego państwa członkowskiego oraz koordynacji takich kontroli przez wyznaczone organy.

2. Prawo dostępu do danych wprowadzonych do SIS II oraz prawo do bezpośredniego przeszukiwania takich danych mogą być wykonywane również przez krajowe organy sądowicze, w tym odpowiedzialne za wszczynanie dochodzeń z oskarżenia publicznego w postępowaniu karnym i dochodzeń sądowych przed wniesieniem aktu oskarżenia, w ramach wykonywania zadań określonych przez ustawodawstwo krajowe, a także przez organy pełniące wobec nich funkcję koordynującą.

3. Ponadto z prawa dostępu do danych, które zostały wprowadzone do SIS II i danych o dokumentach dotyczących osób, które to dane zostały wprowadzone zgodnie z art. 38 ust. 2 lit. d) i e) ► **C1** decyzji 2007/533/WSiSW ◀ oraz z prawa do bezpośredniego przeszukiwania takich danych mogą korzystać organy odpowiedzialne za wydawanie

⁽¹⁾ Dz.U. L 105 z 13.4.2006, str. 1.

▼B

wiz, organy centralne odpowiedzialne za rozpatrywanie wniosków wizowych oraz organy odpowiedzialne za wydawanie dokumentów pobytowych i za wykonywanie przepisów dotyczących obywateli państw trzecich w ramach stosowania dorobku Wspólnoty w zakresie przemieszczania się osób. Dostęp tych organów do danych jest regulowany prawem każdego z państw członkowskich.

4. Organy, o których mowa w niniejszym artykule, są uwzględniane w wykazie, o którym mowa w art. 31 ust. 8.

▼M2*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⁽¹⁾ 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.

⁽¹⁾ 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).

▼ M2

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.

▼ M2

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 ⁽¹⁾ 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.

⁽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).

▼ M2

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 ⁽¹⁾.

▼ B*Artykuł 28***Ograniczenia dostępu**

Użytkownicy mogą mieć dostęp tylko do tych danych, które są im potrzebne do wykonywania ich zadań.

*Artykuł 29***Okres przechowywania wpisów**

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

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

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

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

⁽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).

▼B

5. Po upływie okresu weryfikacji, o którym mowa w ust. 2, wpisy usuwane są automatycznie poza przypadkami, gdy państwo członkowskie, które dokonało wpisu, przekazało do CS-SIS informację o przedłużeniu okresu przechowywania wpisu, zgodnie z ust. 4. CS-SIS automatycznie informuje państwa członkowskie z czteromiesięcznym wyprzedzeniem o zaplanowanym usunięciu danych z systemu.

6. Państwa członkowskie przechowują statystyki dotyczące liczby wpisów, których okres przechowywania został przedłużony zgodnie z ust. 4.

*Artykuł 30***Uzyskanie obywatelstwa a wpisy**

Wpisy dotyczące osoby, która uzyskała obywatelstwo któregośkolwiek z państw, których obywatele mogą korzystać z prawa do swobodnego przepływu w obrębie Wspólnoty, są usuwane po stwierdzeniu lub uzyskaniu przez państwo członkowskie, które dokonało wpisu, informacji zgodnie z art. 34, że dana osoba uzyskała takie obywatelstwo.

ROZDZIAŁ V

OGÓLNE ZASADY PRZETWARZANIA DANYCH*Artykuł 31***Przetwarzanie danych SIS II**

1. Dane, o których mowa w art. 20 mogą być przetwarzane przez państwa członkowskie do celów odmowy pozwolenia na wjazd lub pobyt na ich terytorium.

2. Dane mogą być kopiowane wyłącznie do celów technicznych, pod warunkiem że takie kopiowanie jest niezbędne do przeprowadzenia bezpośredniego wyszukiwania przez organy określone w art. 27. Do takich kopii mają zastosowanie przepisy niniejszego rozporządzenia. Wpisy dokonywane przez jedno państwo członkowskie nie mogą być kopiowane z jego N. SIS II do innych krajowych plików danych.

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

Niezależnie od postanowień akapitu pierwszego tworzenie kopii technicznych przekształczanych w bazy danych istniejące w trybie off-line do użytku organów wizowych jest zakazane po upływie roku od chwili, gdy dany organ został z powodzeniem podłączony do infrastruktury łączności systemu informacji wizowej, który ma zostać przewidziany w przyszłym rozporządzeniu dotyczącym systemu informacji wizowej i wymiany danych pomiędzy państwami członkowskimi na temat wiz, z wyjątkiem kopii sporządzonych do użytku jedynie w sytuacjach awaryjnych, gdy sieć pozostaje niedostępna przez ponad 24 godziny.

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

▼B

4. Prawo dostępu do danych przyznaje się wyłącznie w granicach kompetencji organów krajowych, o których mowa w art. 27, właściwie upoważnionym pracownikom.

5. Danych nie wolno wykorzystywać do celów administracyjnych. Na zasadzie odstępstwa dane wprowadzane zgodnie z niniejszym rozporządzeniem mogą być wykorzystywane – zgodnie z prawem poszczególnych państw członkowskich – przez organy, o których mowa w art. 27 ust. 3, do wykonywania ich zadań.

6. Dane wprowadzone zgodnie z art. 24 niniejszego rozporządzenia oraz dane o dokumentach dotyczących osób wprowadzone na mocy art. 38 ust. 2 lit d) i e) ►**C1** decyzji 2007/533/WSiSW ◀ można wykorzystywać zgodnie z przepisami każdego państwa członkowskiego do celów określonych w art. 27 ust. 3 niniejszego rozporządzenia.

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

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

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

*Artykuł 32***Dane SIS II a pliki krajowe**

1. Art. 31 ust. 2 nie narusza prawa państwa członkowskiego do przechowywania w swoich plikach krajowych danych SIS II, w związku z którymi podjęto działanie na jego terytorium. Dane takie są przechowywane w plikach krajowych przez okres nie dłuższy niż trzy lata, chyba że przepisy szczegółowe prawa krajowego przewidują dłuższy okres ich przechowywania.

2. Art. 31 ust. 2 nie narusza prawa państwa członkowskiego do przechowywania w pliku krajowym danych zawartych w konkretnym wpisie dokonany w SIS II przez to państwo członkowskie.

*Artykuł 33***Informacja w przypadku niewykonania wpisu**

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

▼B*Artykuł 34***Jakość danych przetwarzanych w SIS II**

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

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

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

4. Jeżeli państwa członkowskie w ciągu dwóch miesięcy nie są w stanie osiągnąć porozumienia, państwo członkowskie, które nie dokonało wpisu, przekazuje sprawę Europejskiemu Inspektorowi Ochrony Danych, który wraz z zainteresowanymi krajowymi organami nadzorczymi podejmuje działania mediacyjne.

5. Jeżeli dana osoba twierdzi, że nie jest osobą poszukiwaną na podstawie wpisu, państwa członkowskie wymieniają informacje uzupełniające. Jeżeli wynik kontroli potwierdza, że rzeczywiście chodzi o dwie różne osoby, osoba ta zostaje powiadomiona o przepisach art. 36.

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

*Artykuł 35***Rozróżnianie osób o podobnych cechach**

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

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

▼B

- b) jeżeli kontrola potwierdzi, że osoba, której dotyczy nowy wpis, oraz osoba już ujęta w SIS II to rzeczywiście ta sama osoba, biuro SIRENE stosuje procedurę dokonywania wielokrotnych wpisów, o której mowa w art. 34 ust. 6. Jeżeli kontrola wykaże, że chodzi o dwie różne osoby, biuro SIRENE przyjmuje wniosek o dokonanie drugiego wpisu, dodając informacje niezbędne do uniknięcia błędnej identyfikacji.

*Artykuł 36***Dodatkowe dane wprowadzane w celu rozwiązywania problemów związanych z błędną identyfikacją osób**

1. Jeżeli istnieje ryzyko pomylenia osoby, której faktycznie dotyczy wpis, z osobą, której tożsamość jest przedmiotem pomyłki, państwo członkowskie, które dokonało wpisu, uzupełnia wpis za wyraźną zgodą tej drugiej osoby o dane dotyczące tej drugiej osoby w celu uniknięcia negatywnych skutków błędnej identyfikacji.

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

- a) umożliwienia właściwym organom odróżnienia osoby, której tożsamość jest przedmiotem pomyłki, od osoby, której faktycznie dotyczy wpis;
- b) umożliwienia osobie, której tożsamość jest przedmiotem pomyłki, udowodnienia swojej tożsamości i ustalenie faktu pomylenia tożsamości.

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

- a) nazwisko (nazwiska) i imię (imiona), nazwisko (nazwiska) rodowe, poprzednio używane imiona/nazwiska oraz wszelkie pseudonimy, wpisane oddzielnie, jeśli to możliwe;
- b) wszelkie szczególne obiektywne cechy fizyczne niepodlegające zmianom;
- c) miejsce i data urodzenia;
- d) płeć;
- e) fotografie;
- f) odciski palców;
- g) obywatelstwo (obywatelstwa);
- h) numer dokumentu (numery dokumentów) tożsamości wraz z datą wydania.

▼B

4. Techniczne zasady wpisywania i dalszego przetwarzania danych, o których mowa w ust. 3, są ustalane zgodnie z procedurą, o której mowa w art. 51 ust. 2, bez uszczerbku dla przepisów aktu ustanawiającego organ zarządzający.

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

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

*Artykuł 37***Odsyłacze do innych wpisów**

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

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

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

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

5. Państwo członkowskie może tworzyć odsyłacze zgodnie ze swoimi przepisami krajowymi pod warunkiem przestrzegania zasad określonych w niniejszym artykule.

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

7. Techniczne zasady tworzenia odsyłaczy do innych wpisów są przyjmowane zgodnie z procedurą, o której mowa w art. 51 ust. 2, bez uszczerbku dla przepisów aktu ustanawiającego organ zarządzający.

*Artykuł 38***Cel i okres przechowywania informacji uzupełniających**

1. Państwa członkowskie przechowują odniesienia do decyzji, które są podstawą wpisu, w biurze SIRENE w celu ułatwienia wymiany informacji uzupełniających.
2. Dane osobowe przechowywane w aktach biura SIRENE w wyniku wymiany informacji są przechowywane wyłącznie przez okres wymagany do osiągnięcia celów, w których zostały dostarczone. Są one usuwane najpóźniej po upływie roku od momentu usunięcia związanego z nimi wpisu z SIS II.
3. Ust. 2 nie narusza prawa państwa członkowskiego do przechowywania w plikach krajowych danych dotyczących poszczególnych wpisów, których same dokonały, lub wpisów, w związku z którymi podjęto działania na jego terytorium. Okres przechowywania takich danych we wspomnianych aktach reguluje prawo krajowe.

*Artykuł 39***Przekazywanie danych osobowych stronom trzecim**

Dane przetwarzane w SIS II zgodnie z niniejszym rozporządzeniem nie są przekazywane ani udostępniane państwom trzecim ani organizacjom międzynarodowym.

ROZDZIAŁ VI

OCHRONA DANYCH

*Artykuł 40***Przetwarzanie wrażliwych kategorii danych**

Zabronione jest przetwarzanie danych należących do kategorii wymienionych w art. 8 ust. 1 dyrektywy 95/46/WE.

*Artykuł 41***Prawo dostępu do danych, korekty nieścisłości oraz usunięcia danych wprowadzonych niezgodnie z prawem**

1. Prawo osób do dostępu do danych, które ich dotyczą, wprowadzonych do SIS II zgodnie z niniejszym rozporządzeniem, wykonywane jest zgodnie z prawem państwa członkowskiego, wobec którego powołują się one na to prawo.

▼ B

2. Jeżeli prawo krajowe tak stanowi, krajowy organ nadzorczy decyduje, czy informacje mają być podane do wiadomości oraz zgodnie z jakimi procedurami.
3. Państwo członkowskie, inne niż to, które dokonało wpisu, może przekazać informację dotyczącą takich danych tylko w przypadku, gdy uprzednio umożliwiło państwu członkowskiemu, które dokonało wpisu, zajęcie w tej sprawie stanowiska. Umożliwienie zajęcia stanowiska następuje w drodze wymiany informacji uzupełniających.
4. Informacje nie są przekazywane osobie, której dotyczą dane, jeżeli jest to konieczne do realizacji uprawnionych działań w związku z wpisem lub dla ochrony praw i wolności osób trzecich.
5. Każdy ma prawo do żądania, by dotyczące go dane niezgodne ze stanem faktycznym zostały poprawione, a dotyczące go dane przechowywane z naruszeniem prawa usunięte.
6. Dana osoba informowana jest możliwie szybko, a w każdym razie nie później niż 60 dni od daty złożenia przez nią wniosku o dostęp, lub wcześniej, jeżeli prawo krajowe przewiduje krótszy okres.
7. O działaniach podjętych po skorzystaniu przez daną osobę z prawa do korekty i usunięcia danych, jest ona informowana możliwie szybko, a w każdym razie nie później niż trzy miesiące od daty złożenia przez nią wniosku o korektę lub usunięcie danych lub wcześniej, jeżeli prawo krajowe przewiduje krótszy okres.

*Artykuł 42***Prawo do informacji**

1. Obywatele państwa trzeciego, których dotyczy wpis dokonany zgodnie z niniejszym rozporządzeniem, otrzymują informacje o wpisie zgodnie z art. 10 i 11 dyrektywy 95/46/WE. Informacje te są przekazywane na piśmie wraz z kopią decyzji krajowej, o której mowa w art. 24 ust. 1 i która stanowi podstawę dokonania wpisu lub wraz z odesłaniem do takiej decyzji.
2. Informacje te w żadnym przypadku nie są przekazywane,
 - a) jeżeli
 - (i) dane osobowe nie zostały uzyskane od danego obywatela państwa trzeciego;oraz
 - (ii) przekazanie tych informacji okazuje się niemożliwe lub wymagałoby nieproporcjonalnego nakładu pracy;
 - b) jeżeli dany obywatel państwa trzeciego posiada już te informacje;

▼B

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

*Artykuł 43***Środki odwoławcze**

1. Każdy może wystąpić do sądów lub organów właściwych na mocy prawa krajowego któregośkolwiek z państw członkowskich z wnioskiem o dostęp do informacji, skorygowanie, usunięcie lub uzyskanie informacji lub o odszkodowanie w związku z dotyczącym go wpisem.
2. Państwa członkowskie zobowiązują się wzajemnie do wykonywania ostatecznych decyzji wydanych przez sądy lub organy, o których mowa w ust. 1, bez uszczerbku dla przepisów art. 48.
3. Przepisy dotyczące środków odwoławczych, o których mowa w niniejszym artykule, są poddawane ocenie przez Komisję w terminie do....

*Artykuł 44***Nadzór nad N. SIS II**

1. Organ lub organy wyznaczone w każdym państwie członkowskim, którym powierzono uprawnienia określone w art. 28 dyrektywy 95/46/WE, („krajowy organ nadzorczy”) niezależnie nadzorują, czy dane osobowe zawarte w SIS II są przetwarzane na jego terytorium i przekazywane z jego terytorium zgodnie z prawem oraz nadzorują wymianę i dalsze przetwarzanie informacji uzupełniających.
2. Krajowy organ nadzorczy zapewnia, aby co najmniej co cztery lata przeprowadzany był audyt operacji przetwarzania danych w ramach ich N. SIS II zgodny z międzynarodowymi standardami audytu.
3. Państwa członkowskie zapewniają, by krajowy organ nadzorczy dysponował zasobami wystarczającymi do wykonania zadań powierzonych mu na mocy niniejszego rozporządzenia.

*Artykuł 45***Nadzór nad organem zarządzającym**

1. Europejski Inspektor Ochrony Danych kontroluje, czy działania organu zarządzającego w zakresie przetwarzania danych wykonywane

▼B

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

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

*Artykuł 46***Współpraca krajowych organów nadzorczych z Europejskim Inspektorem Ochrony Danych**

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

2. W zależności od potrzeb i w ramach swoich kompetencji obie strony wymieniają istotne informacje, wspomagają się wzajemnie w przeprowadzaniu kontroli i inspekcji, analizują trudności w zakresie wykładni lub stosowania niniejszego rozporządzenia, badają problemy związane ze sprawowaniem niezależnego nadzoru lub z wykonywaniem praw osób, których dotyczą dane, sporządzają uzgodnione wnioski w sprawie wspólnych rozwiązań problemów oraz upowszechniają wiedzę o uprawnieniach w zakresie ochrony danych.

3. Krajowe organy nadzorcze oraz Europejski Pełnomocnik ds. Ochrony Danych spotykają się w tym celu przynajmniej dwa razy do roku. Koszty tych spotkań i ich obsługa leżą w gestii Europejskiego Inspektora Ochrony Danych. Podczas pierwszego spotkania zostaje przyjęty regulamin wewnętrzny. Metody dalszych prac określone są wspólnie, zależnie od potrzeb. Wspólne sprawozdanie z działalności jest przesyłane co dwa lata Parlamentowi Europejskiemu, Radzie, Komisji i organowi zarządzającemu.

*Artykuł 47***Ochrona danych w okresie przejściowym**

Jeżeli w okresie przejściowym Komisja powierza swoje obowiązki innemu organowi lub organom zgodnie z art. 15 ust. 4, zapewnia ona Europejskiemu Inspektorowi Ochrony Danych prawo oraz możliwość pełnego wykonywania jego zadań, w tym przeprowadzania kontroli na miejscu oraz wykonywania wszelkich innych powierzonych mu uprawnień na mocy art. 47 rozporządzenia (WE) nr 45/2001.



ROZDZIAŁ VII

ODPOWIEDZIALNOŚĆ PRAWNA I SANKCJE

*Artykuł 48***Odpowiedzialność**

1. Każde państwo członkowskie ponosi odpowiedzialność, zgodnie ze swoim prawem krajowym, za wszelkie szkody wyrządzone danej osobie w związku z użytkowaniem N. SIS II. Przepis ten ma również zastosowanie do szkód wyrządzonych przez państwo członkowskie, które dokonało wpisu, jeżeli państwo to wprowadziło dane niezgodne ze stanem faktycznym lub przechowuje dane w sposób niezgodny z prawem.

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

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

*Artykuł 49***Sankcje**

Państwa członkowskie zapewniają, aby wszelkie przypadki nadużycia danych wprowadzonych do SIS II lub wymiany informacji uzupełniających z naruszeniem niniejszego rozporządzenia podlegały skutecznym, proporcjonalnym i odstrasżającym sankcjom, zgodnie z prawem krajowym.

ROZDZIAŁ VIII

PRZEPISY KOŃCOWE

*Artykuł 50***Monitorowanie i statystyka**

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

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

3. Organ zarządzający publikuje co roku statystyki pokazujące liczbę rekordów przypadających na daną kategorię wpisów, liczbę uzyskanych

▼B

w systemie potwierdzeń przypadających na daną kategorię wpisów oraz liczbę wejść do SIS II, ogółem oraz w rozbiciu na poszczególne państwa członkowskie.

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

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

6. Państwa członkowskie dostarczają organowi zarządzającemu i Komisji informacji niezbędnych do sporządzania sprawozdań, o których mowa w ust. 3, 4 i 5.

7. Organ zarządzający dostarcza Komisji informacji niezbędnych do sporządzania ogólnych ocen, o których mowa w ust. 5.

8. W okresie przejściowym, do czasu podjęcia obowiązków przez organ zarządzający, za sporządzanie i przekazywanie sprawozdań, o których mowa w ust. 3 i 4, odpowiedzialna jest Komisja.

*Artykuł 51***Komitet**

1. Komisja jest wspierana przez komitet.

2. W przypadku odesłania do niniejszego ustępu zastosowanie mają art. 5 i 7 decyzji 1999/468/WE, z uwzględnieniem przepisów jej art. 8.

Okres przewidziany w art. 5 ust. 6 decyzji 1999/468/WE wynosi trzy miesiące.

3. Komitet sprawuje swoje funkcje od dnia wejścia w życie niniejszego rozporządzenia.

*Artykuł 52***Zmiany w postanowieniach dorobku Schengen**

1. Z dniem, o którym mowa w art. 55 ust. 2, w kwestiach wchodzących w zakres Traktatu niniejsze rozporządzenie zastępuje artykuły 92–119 Konwencji z Schengen, z wyjątkiem art. 102a tej konwencji.

▼B

2. Z dniem, o którym mowa w art. 55 ust. 2, zastępuje ono także następujące przepisy dorobku Schengen, mające na celu wprowadzenie w życie powyższych artykułów ⁽¹⁾:

- a) decyzja Komitetu Wykonawczego z dnia 14 grudnia 1993 r. w sprawie rozporządzenia finansowego dotyczącego kosztów budowy i eksploatacji systemu informacyjnego Schengen (C. SIS) (SCH/Com-ex (93) 16);
- b) decyzja Komitetu Wykonawczego z dnia 7 października 1997 r. w sprawie rozwoju SIS (SCH/Com-ex (97) 24);
- c) decyzja Komitetu Wykonawczego z dnia 15 grudnia 1997 r. zmieniająca rozporządzenie finansowe w sprawie systemu C. SIS (SCH/Com-ex (97) 35);
- d) decyzja Komitetu Wykonawczego z dnia 21 kwietnia 1998 r. w sprawie C. SIS dla 15/18 przyłączy (SCH/Com-ex (98) 11);
- e) decyzja Komitetu Wykonawczego z dnia 28 kwietnia 1999 r. w sprawie wydatków na budowę C. SIS (SCH/Com-ex (99) 4);
- f) decyzja Komitetu Wykonawczego z dnia 28 kwietnia 1999 r. w sprawie uaktualnienia podręcznika SIRENE (SCH/Com-ex (99) 5);
- g) deklaracja Komitetu Wykonawczego z dnia 18 kwietnia 1996 r. definiująca pojęcie cudzoziemca (SCH/Com-ex (96) dekl. 5);
- h) deklaracja Komitetu Wykonawczego z dnia 28 kwietnia 1999 r. w sprawie struktury SIS (SCH/Com-ex (99) dekl. 2 zmieniona);
- i) decyzja Komitetu Wykonawczego z dnia 7 października 1997 r. w sprawie udziału Norwegii i Islandii w kosztach budowy i eksploatacji C. SIS (SCH/Com-ex (97) 18).

3. W kwestiach objętych zakresem stosowania Traktatu, odesłania do zastąpionych artykułów konwencji z Schengen i odpowiednich przepisów dorobku Schengen mających na celu wykonanie tych artykułów uznaje się za odesłania do niniejszego rozporządzenia.

*Artykuł 53***Uchylenie**

Z dniem, o którym mowa w art. 55 ust. 2, uchyla się rozporządzenie (WE) nr 378/2004, rozporządzenie (WE) nr 871/2004, decyzję 2005/451/WSiSW, decyzję 2005/728/WSiSW i decyzję 2006/628/WE.

⁽¹⁾ Dz.U. L 239 z 22.9.2000, str. 439.

*Artykuł 54***Okres przejściowy i budżet**

1. Wpisy są przenoszone z SIS 1+ do SIS II. Państwa członkowskie zapewniają, traktując priorytetowo wpisy dotyczące osób, by treść wpisów przenoszonych z SIS 1+ do SIS II możliwie szybko i nie później niż w terminie trzech lat od dnia, o którym mowa w art. 55 ust. 2, była zgodna z przepisami niniejszego rozporządzenia. W okresie przejściowym państwa członkowskie mogą nadal stosować postanowienia art. 94 i 96 Konwencji z Schengen do treści wpisów przenoszonych z SIS 1+ do SIS II, z zastrzeżeniem następujących zasad:

- a) jeżeli nastąpi zmiana, uzupełnienie, korekta lub aktualizacja treści wpisu przeniesionego z SIS 1+ do SIS II, państwa członkowskie zapewniają, by wpis był zgodny z przepisami niniejszego rozporządzenia od momentu jego zmiany, uzupełnienia, korekty lub aktualizacji;
- b) jeżeli system potwierdzi istnienie wpisu przeniesionego z SIS 1+ do SIS II, państwa członkowskie sprawdzają natychmiast, czy wpis taki jest zgodny z przepisami niniejszego rozporządzenia, nie opóźniając przy tym podjęcia działań, do których wpis ten obowiązuje.

2. Część budżetu pozostała w dniu określonym zgodnie z art. 55 ust. 2, zatwierdzona zgodnie z art. 119 Konwencji z Schengen, zostanie zwrócona państwom członkowskim. Kwoty podlegające zwrotowi są obliczane na podstawie wpłat państw członkowskich, według decyzji Komitetu Wykonawczego z dnia 14 grudnia 1993 r. w sprawie rozporządzenia finansowego dotyczącego kosztów budowy i eksploatacji systemu informacyjnego Schengen.

3. W okresie przejściowym, o którym mowa w art. 15 ust. 4, odniesienia do organu zarządzającego w niniejszym rozporządzeniu uznaje się za odnoszące się do Komisji.

*Artykuł 55***Wejście w życie, stosowanie i przejście z jednego systemu do drugiego**

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

2. Do państw członkowskich uczestniczących w SIS 1+ ma ono zastosowanie począwszy od dat, które zostaną określone przez Radę na podstawie jednomyślnej decyzji jej członków, reprezentantów rządów państw członkowskich uczestniczących w SIS 1+.

▼B

3. Daty, o których mowa w ust. 2, są ustalane, gdy:
 - a) zostaną przyjęte niezbędne środki wykonawcze;
 - b) wszystkie państwa członkowskie w pełni uczestniczące w SIS 1+ poinformują Komisję, że dokonały uzgodnień technicznych i prawnych niezbędnych do przetwarzania danych zawartych w SIS II oraz do wymiany informacji uzupełniających;
 - c) Komisja ogłosi, że kompleksowe testy przeprowadzane przez Komisję wspólnie z państwami członkowskimi zakończyły się pomyślnie, a organy przygotowawcze Rady dokonają walidacji przedstawionych wyników testów i potwierdzą, że sprawność systemu SIS II jest co najmniej równoważna sprawności osiągniętej przez SIS 1+;
 - d) Komisja dokona niezbędnych uzgodnień technicznych umożliwiających połączenie centralnego SIS II z N. SIS II odnośnych państw członkowskich.
4. Komisja informuje Parlament Europejski o wynikach testu przeprowadzonego zgodnie z ust. 3 lit. c).
5. Każda decyzja Rady podjęta zgodnie z ust. 2 podlega publikacji w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane w państwach członkowskich zgodnie z Traktatem ustanawiającym Wspólnotę Europejską.