

Dokument ten służy wyłącznie do celów informacyjnych i nie ma mocy prawnej. Unijne instytucje nie ponoszą żadnej odpowiedzialności za jego treść. Autentyczne wersje odpowiednich aktów prawnych, włącznie z ich preambułami, zostały opublikowane w Dzienniku Urzędowym Unii Europejskiej i są dostępne na stronie EUR-Lex. Bezpośredni dostęp do tekstów urzędowych można uzyskać za pośrednictwem linków zawartych w dokumencie

► **B**

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)

zmieniona przez:

Dziennik Urzędowy

		nr	strona	data
► <u>M1</u>	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1726 z dnia 14 listopada 2018 r.	L 295	99	21.11.2018
► <u>M2</u>	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r.	L 312	56	7.12.2018

sprostowane przez:

► **C1** Sprostowanie, Dz.U. L 299 z 17.10.2014, s. 33 (2007/533/WSiSW)

**DECYZJA RADY 2007/533/WSiSW**

z dnia 12 czerwca 2007 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 niniejszą decyzją 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 WE odnoszących się do przepływu osób na terytorium państw członkowskich.

*Artykuł 2***Zakres zastosowania**

1. Niniejsza decyzja określa warunki i procedury dokonywania oraz przetwarzania wpisów w SIS II dotyczących osób i przedmiotów oraz wymiany informacji uzupełniających i danych dodatkowych w celach związanych ze współpracą policyjną i sądową w sprawach karnych.

2. Ponadto niniejsza decyzja 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**

1. Na użytek niniejszej decyzji stosuje się następujące definicje:

- a) „wpis” oznacza zbiór danych wprowadzonych do SIS II, umożliwiających właściwym organom zidentyfikowanie osoby lub przedmiotu 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;

▼ B

- (iii) w przypadku niemożności podjęcia wymaganego działania;
 - (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) „dane osobowe” oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dotyczą dane”); osoba możliwa do zidentyfikowania to taka osoba, która może zostać zidentyfikowana bezpośrednio lub pośrednio;
- e) „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.

2. W przypadku odesłania w niniejszej decyzji do przepisów decyzji ramowej 2002/584/WSiSW uznaje się, że zastosowanie mają także odpowiednie postanowienia umów, które Unia Europejska zawarła z państwami trzecimi na podstawie art. 24 i 38 Traktatu UE w celach związanych z wydawaniem osób na podstawie nakazu aresztowania, które przewidują przekazywanie takiego nakazu aresztowania za pośrednictwem systemu informacyjnego Schengen.

*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”),
 - jednorodnego interfejsu krajowego (dalej zwanego „NI-SIS”);
 - 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 zaszyfrowaną sieć wirtualną i wymieniane między biurami SIRENE, o których mowa w art. 7 ust. 2.

▼ B

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 rezerwowi 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.

ROZDZIAŁ II

OBOWIĄZKI PAŃSTW CZŁONKOWSKICH**▼ M2***Artykuł 6***Systemy krajowe**

1. Każde państwo członkowskie odpowiada za utworzenie, funkcjonowanie, utrzymanie i dalsze rozwijanie własnego 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”).

▼B

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 niniejszej decyzji.

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, biuro SIRENE posiada 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. 46 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.

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

4. Szczegółowe zasady wymiany informacji uzupełniających są przyjmowane zgodnie z procedurą określoną w art. 67, 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 ustalone są zgodnie z procedurą, o której mowa w art. 67, bez uszczerbku dla przepisów aktu prawnego powołującego organ zarządzający.

2. Jeżeli państwo członkowskie korzysta z kopii krajowej, jest ono zobowiązane zapewnić — korzystając z usług zapewnianych przez 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.

▼ B*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 sporządzanie 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, 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 niezwłocznie udostępniane krajowym organom nadzorczym, o których mowa w art. 60, 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 niniejszej decyzji (autokontrola).

▼ B

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.

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 niniejszej decyzji, 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 lit. a). 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.

▼ B

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.

*Artykuł 13***Autokontrola****▼ C1**

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

▼ B*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 także 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.

▼ M2

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 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 wieloletnią 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 WE. Komisja zapewnia w szczególności, by delegowanie tych zadań nie wpłynęło niekorzystnie na jakikolwiek system skutecznej kontroli ustanowiony prawem Unii Europejskiej, sprawowanej przez Trybunał Sprawiedliwości, Trybunał Obrachunkowy lub też przez Europejskiego Inspektora Ochrony Danych.

⁽¹⁾ Dz.U. L 248 z 16.9.2002, str. 1.

▼ M2

8. Zarządzanie operacyjne centralnym SIS II obejmuje wszystkie zadania niezbędne do tego, by centralny SIS II działał zgodnie z niniejszą decyzją 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

▼ 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. 61, 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 niniejszej decyzji (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 niniejszej decyzji. 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 niniejszej decyzji, 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 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 Komisji, 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

KATEGORIE DANYCH I UMIESZCZANIE ZNACZNIKÓW*Artykuł 20***Kategorie danych****▼C1**

1. Bez uszczerbku dla art. 8 ust. 1 ani dla przepisów niniejszej decyzji dotyczących przechowywania danych dodatkowych, SIS II zawiera wyłącznie te kategorie danych dostarczanych przez każde z państw członkowskich, jakich wymagają cele określone w art. 26, 32, 34, 36 i 38.

▼B

2. Dane te dzielą się na następujące kategorie:

a) osoby, w odniesieniu do których został wprowadzony wpis;

b) przedmioty, o których mowa w art. 36 i 38.

▼ B

3. Informacje o osobach, w odniesieniu do których dokonano wpisu, nie zawierają innych danych niż:

- a) nazwisko(-a) i imię (imiona), nazwisko(-a) 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(-a);
- 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;
- l) działania, jakie należy podjąć;
- m) odsyłacz lub odsyłacze do innych wpisów dokonanych w SIS II, określone w art. 52;
- n) rodzaj przestępstwa.

4. Techniczne zasady wpisywania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 2 i 3, są ustalane zgodnie z procedurą, o której mowa w art. 67, bez uszczerbku dla przepisów aktu ustanawiającego organ zarządzający.

5. 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 art. 46 ust. 2.

*Artykuł 21***Proporcjonalność**

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

▼ M2

Jeżeli dana osoba lub dany przedmiot są poszukiwane na podstawie wpisu dotyczącego przestępstwa terrorystycznego, 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.

▼B*Artykuł 22***Szczególne zasady dotyczące fotografii i odcisków palców**

Fotografie i odciski palców, o których mowa w art. 20 ust. 3 lit. e) i f), są wykorzystywane pod warunkiem spełnienia następujących wymogów:

- a) fotografie i odciski palców wprowadzane są dopiero po specjalnej kontroli jakości stwierdzającej, czy spełniają minimalny standard jakości danych. Specyfikacja tej specjalnej kontroli jakości jest ustalana zgodnie z procedurą, o której mowa w art. 67, bez uszczerbku dla przepisów aktu ustanawiającego organ zarządzający;
- b) fotografie i odciski palców wykorzystywane są jedynie w celu potwierdzenia tożsamości osoby, która została znaleziona w trakcie wyszukiwania według danych alfanumerycznych przeprowadzonego w SIS II;
- c) jak tylko stanie się to technicznie możliwe, fotografie i odciski palców mogą być także wykorzystywane w celu określenia tożsamości osoby na podstawie znaku biometrycznego. Zanim funkcja ta zostanie wdrożona w SIS II, Komisja przedstawia w sprawozdaniu, czy dostępne i gotowe są niezbędne rozwiązania techniczne; sprawozdanie to konsultowane jest z Parlamentem Europejskim.

*Artykuł 23***Wymóg warunkujący dokonanie wpisu**

1. Wpisów na temat osób nie wolno dokonywać, jeżeli brak jest danych, o których mowa w art. 20 ust. 3 lit. a), d) oraz l), a także w odpowiednich przypadkach w art. 20 ust. 3 lit. k).
2. Wprowadzane są również wszystkie pozostałe dane wymienione w art. 20 ust. 3, o ile są dostępne.

*Artykuł 24***Przepisy ogólne o umieszczaniu znaczników**

1. Jeżeli państwo członkowskie uważa, że wykonanie czynności wymaganych we wpisie dokonany zgodnie z art. 26, 32 lub 36 jest niezgodne z jego prawem krajowym, jego zobowiązaniami międzynarodowymi lub podstawowymi interesami narodowymi, państwo to może zażądać umieszczenia przy wpisie znacznika wskazującego, że działanie, które należy podjąć na podstawie wpisu, nie będzie podjęte na terytorium tego państwa. Znacznik jest dodawany przez biuro SIRENE państwa członkowskiego, które dokonało wpisu.
2. W celu umożliwienia państwom członkowskim żądania umieszczenia znacznika przy wpisie dokonany zgodnie z art. 26, wszystkie państwa członkowskie są – w drodze wymiany informacji uzupełniających — automatycznie informowane o każdym nowym wpisie tej kategorii.

▼B

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

*Artykuł 25***Znaczniki przy wpisach mających prowadzić aresztowania osób w celu ich wydania**

1. Jeżeli zastosowanie ma decyzja ramowa 2002/584/WSiSW, znacznik zapobiegający aresztowaniu jest umieszczany przy wpisie mającym doprowadzić do aresztowania i wydania osoby wyłącznie w przypadku, gdy odmowa organu sądowego właściwego według prawa krajowego w sprawach wykonania europejskiego nakazu aresztowania opiera się na podstawie odmowy wykonania oraz gdy zażądano umieszczenia znacznika.

2. O umieszczenie znacznika przy wpisie mającym doprowadzić do aresztowania osoby w celu jej wydania może wystąpić właściwy według prawa krajowego organ sądowy na podstawie ogólnej instrukcji lub w konkretnej sprawie, jeżeli jest oczywiste, że konieczna będzie odmowa wykonania europejskiego nakazu aresztowania.

ROZDZIAŁ V

WPISY DOTYCZĄCE OSÓB POSZUKIWANYCH W CELU ARESZTOWANIA ICH I WYDANIA LUB EKSTRADYCJI*Artykuł 26***Cele i warunki dokonywania wpisów**

1. Dane osób poszukiwanych w celu aresztowania ich i wydania na podstawie europejskiego nakazu aresztowania lub osób poszukiwanych w celu aresztowania ich i ekstradycji są wprowadzane na wniosek właściwego organu sądowego państwa członkowskiego wydającego nakaz.

2. Dane osób poszukiwanych w celu aresztowania ich i wydania są wprowadzane również na podstawie nakazów aresztowania wydawanych zgodnie z umowami, które Unia Europejska zawarła z państwami trzecimi na podstawie art. 24 i 38 Traktatu UE w celach związanych z wydawaniem osób na podstawie nakazu aresztowania i które przewidują przekazywanie takiego nakazu aresztowania za pośrednictwem Systemu Informacyjnego Schengen.

*Artykuł 27***Dane dodatkowe dotyczące osób poszukiwanych w celu aresztowania ich i wydania**

1. Jeżeli osoba jest poszukiwana w celu aresztowania jej i wydania na podstawie europejskiego nakazu aresztowania, państwo członkowskie wydające nakaz wprowadza do SIS II kopię oryginału europejskiego nakazu aresztowania.

▼B

2. Państwo członkowskie wydające nakaz może wprowadzić do systemu kopię tłumaczenia europejskiego nakazu aresztowania na co najmniej jeden z języków urzędowych instytucji Unii Europejskiej.

*Artykuł 28***Informacje uzupełniające o osobach poszukiwanych w celu aresztowania ich i wydania**

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

*Artykuł 29***Informacje uzupełniające o osobach poszukiwanych w celu aresztowania ich i ekstradycji**

1. Państwo członkowskie, które wprowadziło do SIS II wpis mający doprowadzić do ekstradycji, przekazuje wszystkim państwom członkowskim w drodze wymiany informacji dodatkowe następujące dane:

- a) organ, który wydał wniosek o aresztowanie;
- b) informacja, czy istnieje nakaz aresztowania lub dokument mający identyczny skutek prawny lub podlegający wykonaniu wyrok;
- c) kategoria i kwalifikacja prawna przestępstwa;
- d) opis okoliczności, w których przestępstwo zostało popełnione, w tym czas, miejsce oraz forma udziału osoby, w odniesieniu do której wpis został wprowadzony, w popełnieniu przestępstwa;
- e) w zakresie, w jakim jest to możliwe, konsekwencje popełnienia przestępstwa;
- f) wszelkie inne informacje użyteczne lub niezbędne do tego, by wykonać czynności wymagane we wpisie.

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

*Artykuł 30***Przekształcanie wpisów dotyczących osób poszukiwanych w celu aresztowania ich i wydania lub ekstradycji**

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

▼B*Artykuł 31***Wykonanie działania na podstawie wpisu dotyczącego osoby poszukiwanej w celu aresztowania jej i wydania lub ekstradycji**

1. W przypadkach, w których ma zastosowanie decyzja ramowa 2002/584/WSiSW, wpis dokonany w SIS II zgodnie z art. 26 w połączeniu z danymi dodatkowymi, o których mowa w art. 27, stanowią europejski nakaz aresztowania wydany zgodnie z decyzją ramową 2002/584/WSiSW i mają taki sam skutek.

2. Jeżeli decyzja ramowa 2002/584/WSiSW nie ma zastosowania, wpis dokonany w SIS II zgodnie z art. 26 i art. 29 ma taki sam skutek prawny, co wniosek o tymczasowe aresztowanie wydany na podstawie art. 16 Europejskiej konwencji o ekstradycji z dnia 13 grudnia 1957 r. lub art. 15 Traktatu o unii Beneluksu dotyczącego ekstradycji i wzajemnej pomocy w sprawach karnych z dnia 27 czerwca 1962 r.

ROZDZIAŁ V

WPISY DOTYCZĄCE OSÓB ZAGINIONYCH*Artykuł 32***Cele i warunki dokonywania wpisów**

1. Dane osób zaginionych, które powinny być objęte ochroną lub osób, których miejsce przebywania należy ustalić, są wprowadzane do SIS II na wniosek właściwego organu państwa członkowskiego dokonującego wpisu.

2. Wprowadzane mogą być następujące kategorie osób zaginionych:

a) osoby zaginione, które powinny być objęte ochroną:

- (i) dla ich własnej ochrony;
- (ii) w celu zapobiegania zagrożeniom oraz;

b) osoby zaginione, które nie muszą być objęte ochroną.

3. Ustęp 2 lit. a) ma zastosowanie wyłącznie do osób, które muszą zostać przymusowo umieszczone w odpowiedniej placówce w wyniku decyzji podjętej przez właściwy organ.

4. Ustęp 1, 2 i 3 mają zastosowanie w szczególności do nieletnich.

5. Państwa członkowskie zapewniają, by dane wprowadzane do SIS II wskazywały, do której z kategorii wymienionych w ust. 2 należy dana zaginiona osoba.

*Artykuł 33***Wykonanie działań na podstawie wpisu**

1. W przypadku odnalezienia osoby, o której mowa w art. 32, właściwe organy powiadamiają, z zastrzeżeniem ust. 2, państwo członkowskie, które dokonało wpisu o miejscu pobytu tej osoby. Organy te, w przypadkach, o których mowa w art. 32 ust. 2 lit. a), mogą umieścić tę osobę w bezpiecznym miejscu, aby uniemożliwić jej kontynuowanie podróży, jeżeli uprawnia je do tego prawo krajowe.

▼B

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

ROZDZIAŁ VII

WPISY DOTYCZĄCE OSÓB, KTÓRYCH OBECNOŚĆ JEST WYMAGANA DO CELÓW PROCEDURY SĄDOWEJ*Artykuł 34***Cele i warunki dokonywania wpisów**

Aby zapewnić informację o miejscu zamieszkania lub pobytu, państwa członkowskie wprowadzają do SIS II na wniosek właściwego organu dane dotyczące:

- a) świadków;
- b) osób wezwanych do stawiennictwa przed organami sądowymi w związku z postępowaniem karnym lub w tym celu poszukiwanych, aby złożyły wyjaśnienia w sprawie czynów, za które są ścigane;
- c) osób, którym ma zostać doręczony wyrok sądowy lub inne dokumenty związane z postępowaniem karnym, po to by złożyły wyjaśnienia w sprawie czynów, za które są ścigane;
- d) osób, którym ma zostać doręczone wezwanie do stawienia się w celu odbycia kary pozbawienia wolności.

*Artykuł 35***Wykonanie działania na podstawie wpisu**

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

ROZDZIAŁ VIII

WPISY DOTYCZĄCE OSÓB LUB PRZEDMIOTÓW WPROWADZANE W CELU PRZEPROWADZANIA KONTROLI NIEJAWNYCH LUB KONTROLI SZCZEGÓLNYCH*Artykuł 36***Cele i warunki dokonywania wpisów**

1. Dane osób lub pojazdów, jednostek pływających, statków powietrznych i kontenerów są wprowadzane zgodnie z prawem krajowym państwa członkowskiego, które dokonuje wpisu, do celów kontroli niejawnych lub kontroli szczególnych zgodnie z art. 37 ust. 4.
2. Wpisu takiego można dokonać w celu ścigania przestępstw oraz zapobiegania zagrożeniom bezpieczeństwa publicznego:
 - a) jeżeli istnieją wyraźne oznaki, że dana osoba ma zamiar popełnić lub popełnia poważne przestępstwo, takie jak przestępstwa, o których mowa w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW; lub

▼B

b) jeżeli ogólna ocena danej osoby, zwłaszcza w świetle wcześniej popełnionych przestępstw, daje powód do przypuszczenia, że osoba ta będzie popełniać także w przyszłości poważne przestępstwa, takie jak przestępstwa, o których mowa w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW.

3. Ponadto wpisu można dokonać zgodnie z prawem krajowym na wniosek organów odpowiedzialnych za bezpieczeństwo narodowe, jeżeli istnieją konkretne przesłanki wskazujące, że informacje określone w art. 37 ust. 1 są niezbędne do zapobieżenia poważnemu zagrożeniu stwarzanemu przez daną osobę lub innym poważnym zagrożeniom wewnętrznego i zewnętrznego bezpieczeństwa narodowego. Państwo członkowskie dokonujące wpisu zgodnie z niniejszym ustępem powiadamia o tym pozostałe państwa członkowskie. Każde państwo członkowskie określa, którym organom przekazywane są takie informacje.

4. Wpisy dotyczące pojazdów, jednostek pływających, statków powietrznych i kontenerów mogą być dokonywane, jeżeli istnieją wyraźne oznaki, że są one związane z poważnymi przestępstwami, o których mowa w ust. 2, lub z poważnymi zagrożeniami, o których mowa w ust. 3.

*Artykuł 37***Wykonanie działania na podstawie wpisu**

1. W celu przeprowadzania kontroli niejawnych lub kontroli szczególnych wszystkie lub niektóre z poniższych informacji są gromadzone i przekazywane organowi dokonującemu wpisu, gdy na obszarze państwa członkowskiego prowadzone są kontrole graniczne lub inne kontrole policyjne i celne:

- a) fakt odnalezienia osoby lub pojazdu, jednostki pływającej, statku powietrznego lub kontenera, których dotyczy wpis;
- b) miejsce, czas lub przyczyny kontroli;
- c) trasa i cel podróży;
- d) osoby towarzyszące danej osobie lub osoby przewożone pojazdem, jednostką pływającą lub statkiem powietrznym, co do których istnieją uzasadnione podejrzenia, że pozostają one w związku z osobami, których dotyczy wpis;
- e) wykorzystane: pojazd, jednostka pływająca, statek powietrzny lub kontener;
- f) przewożone przedmioty;
- g) okoliczności, w jakich osoba lub pojazd, jednostka pływająca, statek powietrzny lub kontener zostały znalezione.

2. Informacje określone w ust. 1 są przekazywane w drodze wymiany informacji uzupełniających.

3. W celu uzyskania informacji, o których mowa w ust. 1, państwa członkowskie podejmują niezbędne kroki dla zachowania niejawnego charakteru takiej kontroli.

4. Podczas kontroli szczególnych osoby, pojazdy, jednostki pływające, statki powietrzne, kontenery oraz przewożone przedmioty mogą zostać przeszukane zgodnie z prawem krajowym w celach, o których mowa w art. 36. Jeżeli kontrole szczególne nie są dopuszczalne w świetle prawa państwa członkowskiego, są one automatycznie zastępowane w tym państwie członkowskim kontrolami niejawnymi.

▼B

ROZDZIAŁ IX

**WPISY DOTYCZĄCE PRZEDMIOTÓW PRZEZNACZONYCH DO
ZAJĘCIA LUB WYKORZYSTANIA JAKO DOWÓD
W POSTĘPOWANIU KARNYM***Artykuł 38***Cele i warunki dokonywania wpisów**

1. Dane dotyczące przedmiotów poszukiwanych w celu ich zajęcia lub wykorzystania jako dowód w postępowaniu karnym są wprowadzane do SIS II.
2. Wprowadza się następujące kategorie łatwych do zidentyfikowania przedmiotów:
 - a) pojazdy silnikowe o pojemności skokowej przekraczającej 50 cm³, jednostki pływające i statki powietrzne;
 - b) przyczepy i naczepy o masie własnej przekraczającej 750 kg, przyczepy turystyczne, urządzenia przemysłowe, silniki przyczepne i kontenery;
 - c) broń palna;
 - d) blankiety dokumentów urzędowych, które zostały skradzione, przywłaszczone lub utracone;
 - e) wydane dokumenty tożsamości, takie jak: paszporty, dowody tożsamości, prawa jazdy, dokumenty pobytowe i dokumenty podróży, które zostały skradzione, przywłaszczone, utracone lub unieważnione;
 - f) dowody rejestracyjne i tablice rejestracyjne pojazdów, które zostały skradzione, przywłaszczone, utracone lub unieważnione;
 - g) banknoty (o spisanych numerach);
 - h) papiery wartościowe i środki płatnicze, takie jak: czeki, karty kredytowe, obligacje, akcje i dokumenty potwierdzające udział, które zostały skradzione, przywłaszczone, utracone lub unieważnione.
3. Techniczne zasady wpisywania, aktualizowania, usuwania i przeszukiwania danych, o których mowa w ust. 2, są określane zgodnie z procedurą, o której mowa w art. 67, bez uszczerbku dla przepisów aktu ustanawiającego organ zarządzający.

*Artykuł 39***Wykonanie działania na podstawie wpisu**

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



ROZDZIAŁ X

PRAWO DO DOSTĘPU I PRZECHOWYWANIE WPISÓW

*Artykuł 40***Organy uprawnione do dostępu do wpisów**

1. Dostęp do danych wprowadzonych do SIS II oraz prawo do ich przeszukiwania bezpośrednio lub w kopii danych SIS II są zastrzeżone wyłącznie dla organów odpowiedzialnych za:

a) kontrole graniczne, 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) inne kontrole policyjne i celne prowadzone na terytorium danego państwa członkowskiego, koordynację 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 sądowe — w tym organy 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 funkcje koordynującą.

3. Organy, o których mowa w niniejszym artykule, są uwzględniane w wykazie, o którym mowa w art. 46 ust. 8.

*Artykuł 41***Dostęp Europolu do danych zawartych w SIS II**

1. W ramach swojego mandatu Europejski Urząd Policji (Europol) ma prawo dostępu do danych wprowadzonych do SIS II zgodnie z art. 26, 36 i 38 oraz do bezpośredniego ich przeszukiwania.

2. Jeżeli podczas przeszukiwania danych Europol stwierdzi istnienie wpisu w SIS II, informuje o tym — metodami określonymi w konwencji o Europolu — państwo członkowskie, które dokonało wpisu.

3. Wykorzystanie informacji uzyskanych w wyniku przeszukiwania danych SIS II wymaga zgody danego państwa członkowskiego. Jeżeli to państwo członkowskie pozwoli na wykorzystanie takich informacji, to posługiwanie się nimi podlega postanowieniom konwencji o Europolu. Europol może przekazać takie informacje państwom trzecim i organom trzecim wyłącznie za zgodą danego państwa członkowskiego.

4. Europol może wystąpić o przekazanie przez dane państwo członkowskie dalszych informacji zgodnie z postanowieniami konwencji o Europolu.

⁽¹⁾ Dz.U. L 105 z 13.4.2006, str. 1.

▼ B

5. Europol:
 - a) prowadzi rejestr wszystkich przypadków uzyskania dostępu i przeprowadzonych przez siebie wyszukiwań, zgodnie z postanowieniami art. 12;
 - b) bez uszczerbku dla ust. 4 i 5, nie podłącza części SIS II ani też nie przenosi danych, które są w tych częściach zawarte i które zostały mu udostępnione, do jakiegokolwiek komputerowego systemu gromadzenia i przetwarzania danych stosowanego przez Europol lub w tym urzędzie, a także nie pobiera ani nie kopiuje w inny sposób jakichkolwiek części SIS II;
 - c) ogranicza dostęp do danych wprowadzonych do SIS II w taki sposób, by korzystali z niego tylko specjalnie uprawnieni pracownicy Europolu;
 - d) przyjmuje i stosuje środki przewidziane w art. 10 i 11;
 - e) zapewnia wspólnemu organowi nadzorczemu, ustanowionemu na mocy art. 24 konwencji o Europolu, możliwość sprawdzenia, w jaki sposób Europol korzysta z prawa dostępu do danych wprowadzonych do SIS II i ich przeszukiwania.

*Artykuł 42***Dostęp Eurojustu do danych zawartych w SIS II**

1. Krajowi przedstawiciele oddelegowani do Eurojustu oraz ich asystenci w ramach swojego mandatu mają prawo do dostępu do danych wprowadzonych do SIS II zgodnie z art. 26, 32, 34 i 38 oraz do przeszukiwania tych danych.
2. Jeżeli podczas przeszukiwania danych oddelegowany do Eurojustu krajowy przedstawiciel stwierdzi istnienie wpisu w SIS II, informuje o tym państwo członkowskie, które dokonało wpisu. Informacje uzyskane w wyniku takiego wyszukiwania mogą być przekazywane państwom trzecim i organom trzecim jedynie za zgodą państwa członkowskiego, które dokonało wpisu.
3. Przepisy niniejszego artykułu nie mogą być interpretowane jako modyfikacja przepisów decyzji 2002/187/WSiSW dotyczących ochrony danych i odpowiedzialności prawnej za wszelkie nieuprawnione lub nieprawidłowe przetwarzanie takich danych przez krajowych przedstawicieli oddelegowanych do Eurojustu lub ich asystentów, ani też jako modyfikacja uprawnień wspólnego organu nadzorczego, ustanowionego na mocy tej decyzji.
4. Każdy przypadek uzyskania dostępu i przeprowadzenia wyszukiwania przez krajowego przedstawiciela oddelegowanego do Eurojustu lub jego asystenta zostaje zarejestrowany zgodnie z art. 12; rejestracji podlega również każde wykorzystanie przez nich danych, do których uzyskali dostęp.
5. Żadne części SIS II nie mogą być podłączane, a zawarte w nich dane, udostępniane krajowym przedstawicielom i ich asystentom, nie mogą być przenoszone, do jakiegokolwiek komputerowego systemu gromadzenia i przetwarzania danych stosowanego przez Eurojust lub w tym urzędzie, nie wolno też pobierać żadnych części SIS II.

▼B

6. Dostęp do danych wprowadzonych do SIS II jest zastrzeżony dla krajowych przedstawicieli i ich asystentów i nie może być rozszerzony na pracowników Eurojustu.

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

*Artykuł 43***Zakres dostępu**

Użytkownicy, w tym Europol, krajowi przedstawiciele oddelegowani do Eurojustu i ich asystenci mogą mieć dostęp wyłącznie do tych danych, które są im potrzebne do wykonywania ich zadań.

*Artykuł 44***Okres przechowywania wpisów dotyczących osób**

1. Wpisy dotyczące osób wprowadzane do SIS II zgodnie z niniejszą decyzją są przechowywane wyłącznie przez okres konieczny do 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. W przypadku wpisów dotyczących osób, które zostały dokonane zgodnie z art. 36, okres ten wynosi rok.

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

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 45***Okres przechowywania wpisów dotyczących przedmiotów**

1. Wpisy dotyczące przedmiotów wprowadzane do SIS II zgodnie z niniejszą decyzją są przechowywane wyłącznie przez okres konieczny do osiągnięcia celów, w których zostały wprowadzone.

▼B

2. Wpisy dotyczące przedmiotów wprowadzone zgodnie z art. 36 przechowywane są przez okres nieprzekraczający pięciu lat.
3. Wpisy dotyczące przedmiotów wprowadzone zgodnie z art. 38 przechowywane są przez okres nieprzekraczający dziesięciu lat.
4. Okresy przechowywania danych określone w ust. 2 i 3 mogą być przedłużone, o ile wymagają tego cele, w których dokonano wpisu. W takim przypadku ust. 2 i 3 mają zastosowanie również do przedłużenia okresu przechowywania.

ROZDZIAŁ XI

OGÓLNE ZASADY PRZETWARZANIA DANYCH

*Artykuł 46***Przetwarzanie danych SIS II**

1. Państwa członkowskie mogą przetwarzać dane określone w art. 20, 26, 32, 34, 36 i 38 wyłącznie w celach, jakie zostały określone dla każdej z kategorii wpisów, o których mowa w tych artykułach.
 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. 40. Do takich kopii mają zastosowanie przepisy niniejszej decyzji. 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.
- Państwa członkowskie prowadzą aktualny spis takich kopii, który udostępniają ich krajowemu organowi nadzorcemu i zapewniają, by w odniesieniu do takich kopii stosowane były przepisy niniejszej decyzji, a w szczególności przepisy art. 10.
4. Prawo dostępu do danych przyznaje się wyłącznie w granicach kompetencji organów krajowych, o których mowa w art. 40, właściwie upoważnionym pracownikom.
 5. W odniesieniu do wpisów, o których mowa w art. 26, 32, 34, 36 i 38 niniejszej decyzji, każdy przypadek przetwarzania zawartych w nich informacji do celów innych niż te, w których wpisy te zostały dokonane w SIS II, musi być związany z konkretną sprawą i uzasadniony potrzebą, by zapobiec bezpośredniemu poważnemu zagrożeniu porządku publicznego oraz bezpieczeństwa publicznego, poważnymi względami bezpieczeństwa narodowego lub koniecznością zapobieżenia poważnym przestępstwom. W tym celu należy wcześniej uzyskać zgodę państwa członkowskiego dokonującego wpisu.
 6. Dane nie mogą być wykorzystywane do celów administracyjnych.

▼ B

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 niniejszą decyzją, 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 Unii Europejskiej nie określa szczegółowych przepisów, dane wprowadzane do N.SIS II podlegają prawu każdego państwa członkowskiego.

*Artykuł 47***Dane SIS II a pliki krajowe**

1. Artykuł 46 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. Artykuł 46 ust. 2 nie narusza prawa państwa członkowskiego do przechowywania w pliku krajowym danych zawartych w konkretnym wpisie dokonanym w SIS II przez to państwo członkowskie.

*Artykuł 48***Informacja w przypadku niewykonania wpisu**

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

*Artykuł 49***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, które dokonało wpisu, sprawdza te informacje oraz, jeśli to konieczne, niezwłocznie koryguje lub usuwa zakwestionowane dane.

▼B

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. 51.

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 50***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) 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. 49 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 51***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 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

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(-a) i imię (imiona), nazwisko(-a) 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(-a);

h) numer(-y) dokumentu(-ów) tożsamości wraz z datą wydania.

4. Techniczne zasady wpisywania i dalszego przetwarzania danych, o których mowa w ust. 3, są ustalane zgodnie z procedurą, o której mowa w art. 67, 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 52***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 niniejszej decyzji. Organy nieposiadające prawa dostępu do niektórych kategorii wpisów nie mogą widzieć odsyłacza do wpisu, do którego nie mają dostępu.

▼ B

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 oraz 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. 67, bez uszczerbku dla przepisów aktu ustanawiającego organ zarządzający.

*Artykuł 53***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. Ustęp 2 nie narusza prawa państwa członkowskiego do przechowywania w plikach krajowych danych dotyczących poszczególnych wpisów, których same dokonały, lub wpisów, w związku z którymi podjęto działania na jego terytorium. Okres przechowywania takich danych we wspomnianych aktach reguluje prawo krajowe.

*Artykuł 54***Przekazywanie danych osobowych stronom trzecim**

Dane osobowe przetwarzane w SIS II zgodnie z niniejszą decyzją nie są przekazywane ani udostępniane państwu trzecim ani organizacjom międzynarodowym.

*Artykuł 55***Wymiana z Interpolem danych na temat skradzionych, przywłaszczonych, utraconych lub unieważnionych paszportów**

1. W drodze odstępstwa od art. 54, wprowadzone do SIS II informacje o numerze, kraju wystawienia i typie paszportów skradzionych, przywłaszczonych, utraconych lub unieważnionych mogą być wymieniane z członkami Interpolu poprzez ustanowienie połączenia pomiędzy SIS II a bazą Interpolu zawierającą dane skradzionych lub utraconych dokumentów podróży, o ile zostanie zawarta umowa między Interpolem a Unią Europejską. Umowa ta musi zawierać zastrzeżenie, że przekazanie danych wprowadzonych przez dane państwo członkowskie zależy od zgody tego państwa członkowskiego.

▼B

2. Umowa, o której mowa w ust. 1, przewiduje, że wymieniane dane są dostępne wyłącznie dla członków Interpolu z państw, które zapewniają odpowiedni poziom ochrony danych osobowych. Przed zawarciem tej umowy Rada zasięga opinii Komisji co do adekwatności poziomu ochrony danych osobowych oraz poszanowania podstawowych praw i wolności w odniesieniu do automatycznego przetwarzania danych osobowych przez Interpol i przez państwa, które oddelegowały swoich przedstawicieli do Interpolu.

3. Umowa, o której mowa w ust. 1, może także przewidywać dostęp państw członkowskich za pośrednictwem SIS II do danych z bazy Interpolu zawierającej dane skradzionych lub utraconych dokumentów podróży, zgodnie z odpowiednimi przepisami niniejszej decyzji dotyczącymi wpisów do SIS II na temat skradzionych, przywłaszczonych, utraconych lub unieważnionych paszportów.

ROZDZIAŁ XII

OCHRONA DANYCH*Artykuł 56***Przetwarzanie wrażliwych kategorii danych**

Zabronione jest przetwarzanie danych należących do kategorii wymienionych w art. 6 zdanie pierwsze Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych.

*Artykuł 57***Zastosowanie konwencji Rady Europy o ochronie danych**

Dane osobowe przetwarzane na użytek niniejszej decyzji podlegają ochronie zgodnie z Konwencją Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych wraz z jej późniejszymi zmianami.

*Artykuł 58***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 niniejszą decyzją wykonywane jest zgodnie z prawem państwa członkowskiego, wobec którego osoby te powołują się na to prawo.

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.

▼B

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 59***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. 64.
3. Przepisy dotyczące środków odwoławczych, o których mowa w niniejszym artykule, są poddawane ocenie przez Komisję w terminie do dnia 23 sierpnia 2009 r.

*Artykuł 60***Nadzór nad N.SIS II**

1. Każde państwo członkowskie zapewnia, aby niezależny organ („krajowy organ nadzorczy”) niezależnie nadzorował, czy dane osobowe zawarte w SIS II są przetwarzane na jego terytorium i przekazywane z jego terytorium zgodnie z prawem oraz by nadzorował 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 niniejszej decyzji.

*Artykuł 61***Nadzór nad organem zarządzającym**

1. Europejski Inspektor Ochrony Danych kontroluje, czy działania organu zarządzającego w zakresie przetwarzania danych wykonywane są zgodnie z niniejszą decyzją. 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 umożliwia się organowi zarządzającemu przedstawienie uwag.

*Artykuł 62***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 w przeprowadzaniu kontroli i inspekcji, analizują trudności w zakresie wykładni i stosowania niniejszej decyzji, badają problemy związane ze sprawowaniem niezależnego nadzoru lub wykonywaniem praw osób, których dotyczą dane, sporządzają uzgodnione propozycje 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 63***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 XIII

ODPOWIEDZIALNOŚĆ PRAWNA I SANKCJE*Artykuł 64***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 niniejszej decyzji.
3. W przypadku naruszenia przez państwo członkowskie swoich obowiązków wynikających z niniejszej decyzji i spowodowania tym samym szkody w SIS II ponosi ono odpowiedzialność za tę szkodę, chyba że organ zarządzający lub inne państwa członkowskie uczestniczące w SIS II nie podjęły rozsądnych kroków, by zapobiec wystąpieniu szkody lub zminimalizować jej rozmiar.

*Artykuł 65***Sankcje**

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

ROZDZIAŁ XIV

PRZEPISY KOŃCOWE*Artykuł 66***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 w systemie potwierżeń przypadających na daną kategorię wpisów oraz liczbę wejść do SIS II — ogółem oraz w rozbiciu na poszczególne państwa członkowskie.

▼B

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 niniejsza decyzja stosowana 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.

*Artykuł 67***Komitet regulacyjny**

1. W przypadku odesłania do niniejszego artykułu Komisja wspierana jest przez komitet regulacyjny składający się z przedstawicieli państw członkowskich, któremu przewodniczy przedstawiciel Komisji. Przedstawiciel Komisji przedkłada komitetowi projekt dotyczący środków, jakie należy podjąć. Komitet opiniuje projekt w terminie, który może zostać określony przez przewodniczącego, w zależności od pilności sprawy. Opinia ta jest przyjmowana większością głosów określoną w art. 205 ust. 2 Traktatu WE, przewidzianą dla decyzji, które Rada przyjmuje na wniosek Komisji. Głosy przedstawicieli państw członkowskich w komitecie oblicza się w sposób określony w tym artykule. Przewodniczący nie bierze udziału w głosowaniu.

2. Na podstawie propozycji przewodniczącego komitet przyjmuje regulamin, przygotowany w oparciu o standardowy regulamin opublikowany w *Dzienniku Urzędowym Unii Europejskiej*.

3. Komisja podejmuje zamierzone środki, jeżeli są one zgodne z opinią komitetu. Jeżeli zamierzone środki nie są zgodne z opinią komitetu lub jeżeli opinia nie została wydana, Komisja bezzwłocznie przedstawia Radzie wniosek w sprawie środków, które mają zostać podjęte.

4. W sprawie tego wniosku Rada może stanowić kwalifikowaną większością głosów w terminie dwóch miesięcy od daty jego otrzymania. Jeżeli w tym okresie Rada wyrazi kwalifikowaną większością sprzeciw wobec wniosku, Komisja bada go ponownie. Komisja może przedstawić Radzie zmieniony wniosek, ponownie przedstawić swój wniosek lub przedstawić wniosek w sprawie aktu prawnego. Jeśli w powyższym terminie Rada nie przyjęła proponowanego aktu wykonawczego ani nie wyraziła sprzeciwu wobec wniosku w sprawie środków wykonawczych, Komisja przyjmuje proponowane środki wykonawcze.

▼B

5. Komitet, o którym mowa w ust. 1, pełni obowiązki od dnia 23 sierpnia 2007 r.

*Artykuł 68***Zmiany w postanowieniach prawnego dorobku Schengen****▼C1**

1. Z dniem, o którym mowa w art. 71 ust. 2, w kwestiach wchodzących w zakres Traktatu UE niniejsza decyzja zastępuje art. 64 i 92–119 konwencji z Schengen, z wyjątkiem art. 102a tej konwencji.

▼B

►C1 2. Z dniem, o którym mowa w art. 71 ust. 2, w kwestiach objętych zakresem stosowania Traktatu UE niniejsza decyzja zastępuje 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 przyłążeń (SCH/Com-ex (98) 11);
- e) decyzja Komitetu Wykonawczego z dnia 25 kwietnia 1997 r. w sprawie udzielenia zamówienia na sporządzenie opracowania wstępnego dla SIS II (SCH/Com-ex (97) 2 zm. 2);
- f) decyzja Komitetu Wykonawczego z dnia 28 kwietnia 1999 r. w sprawie wydatków na budowę C.SIS (SCH/Com-ex (99) 4);
- g) decyzja Komitetu Wykonawczego z dnia 28 kwietnia 1999 r. w sprawie uaktualnienia podręcznika SIRENE (SCH/Com-ex (99) 5);
- h) deklaracja Komitetu Wykonawczego z dnia 18 kwietnia 1996 r. definiująca pojęcie cudzoziemca (SCH/Com-ex (96) dekl. 5);
- i) deklaracja Komitetu Wykonawczego z dnia 28 kwietnia 1999 r. w sprawie struktury SIS (SCH/Com-ex (99) dekl. 2 zmieniona);
- j) 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 UE odesłania do zastąpionych artykułów konwencji z Schengen i odpowiednich przepisów dorobku Schengen mających na celu wykonanie tych artykułów uznaje się za odesłania do niniejszej decyzji.

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

▼B*Artykuł 69***Uchylenie**

Z dniem, o którym mowa w art. 71 ust. 2, uchyla się decyzję 2004/201/WSiSW, decyzję 2005/211/WSiSW, decyzję 2005/719/WSiSW, decyzję 2005/727/WSiSW, decyzję 2006/228/WSiSW, decyzję 2006/229/WSiSW i decyzję 2006/631/WSiSW.

*Artykuł 70***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. 71 ust. 2, była zgodna z przepisami niniejszej decyzji. W okresie przejściowym państwa członkowskie mogą nadal stosować postanowienia art. 94, 95, 97–100 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 niniejszej decyzji 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 niniejszej decyzji, nie opóźniając przy tym podjęcia działań, do których wpis ten obliguje.

2. Część budżetu pozostała w dniu określonym zgodnie z art. 71 ust. 2, zatwierdzona zgodnie z art. 119 konwencji z Schengen, zostanie zwrócona państwu 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 niniejszej decyzji uznaje się za odnoszące się do Komisji.

*Artykuł 71***Wejście w życie, stosowanie i przejście z jednego systemu do drugiego**

1. Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej 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*.