

Bruksela, 4 lipca 2017 r.
(OR. en)

6261/17

DAPIX 50
ENFOPOL 62
CT 65
ENFOCUSTOM 33
CRIMORG 28
SCHENGEN 7
VISA 47
SIRIS 25
COPEN 43
ASIM 13
FRONT 61
COMIX 115
JAI 112

NOTA

Od:	Prezydencja
Do:	Grupa Robocza ds. Wymiany Informacji i Ochrony Danych (DAPIX)
Nr poprz. dok.:	11800/1/16 REV 1
Dotyczy:	Podręcznik dotyczący wymiany informacji między organami ścigania

1. Wprowadzenie

Podręcznik dotyczący wymiany informacji między organami ścigania stanowi uzupełnienie podręcznika operacji transgranicznych (dok. 10505/4/09 REV). Zarówno treść, jak i struktura podręcznika oraz zestawień informacyjnych dotyczących poszczególnych państw zostały zatwierdzone przez grupę roboczą DAPIX w ramach strategii w zakresie zarządzania informacjami do celów ochrony bezpieczeństwa wewnętrznego UE, aby wspomagać, ukierunkowywać i ułatwiać transgraniczną wymianę informacji.

W celu zwiększenia wartości praktycznej tego podręcznika zostaną udostępnione jego tłumaczenia na wszystkie języki urzędowe Unii. Ponadto podręcznik będzie uaktualniany dwa razy do roku, jeśli okaże się to niezbędne w świetle nowych aktów prawnych lub doświadczeń praktycznych. Obecna wersja uwzględnia przede wszystkim rozporządzenie w sprawie Europolu oraz dane kontaktowe. Te dane kontaktowe są regularnie aktualizowane przez państwa członkowskie i przedstawiane w zestawieniach informacyjnych dotyczących poszczególnych państw. Zestawienia te są obecnie wydawane jako addendum do niniejszego podręcznika.

2. Cel podręcznika

Podręcznik jest pomyślany przede wszystkim jako narzędzie dla funkcjonariuszy policji zajmujących się współpracą międzynarodową, w szczególności dla tzw. **operatorów pojedynczych punktów kontaktowych**. W związku z tym powinien on być jak najbardziej przyjazny dla użytkownika i kompleksowy.

Podręcznik ma dostarczyć informacji i ułatwić **przebieg rutynowej współpracy** między różnymi organami państw członkowskich zaangażowanymi w wymianę informacji policyjnych na szczeblu krajowym i międzynarodowym, do celów szkoleniowych i do ułatwienia podejmowania lepiej umotywowanych decyzji w przypadku transgranicznego pozyskiwania informacji i ich wymiany.

Podręcznik zawiera **przegląd wszystkich unijnych systemów, podstaw prawnych i instrumentów wymiany informacji** dostępnych organom ścigania państw członkowskich. W ten sposób użytkownik zyskuje pełną informację o dostępnych opcjach przy podejmowaniu decyzji dotyczących sposobu pozyskiwania lub przekazywania informacji w kontekście transgranicznym.

Podręcznik uzupełniają **zestawienia informacyjne dotyczące poszczególnych państw** – przedstawione w addendum – które zawierają odpowiednie dane kontaktowe i informacje objęte transgraniczną wymianą informacji. Regularnie aktualizując zestawienia informacyjne, państwa członkowskie wypełnią wiele zobowiązań w zakresie powiadamiania, nałożonych na nie na mocy różnych instrumentów. Zestawienia informacyjne dotyczące poszczególnych państw powinny ułatwić zarządzanie niezbędnymi informacjami i ich odnajdywanie.

Podręcznik obejmuje te zestawienia informacyjne dotyczące poszczególnych państw i istotne informacje praktyczne na temat decyzji ramowej Rady 2006/960/WSiSW („szwedzka decyzja ramowa”) oraz zastępuje wcześniejsze wytyczne dotyczące szwedzkiej decyzji ramowej (9512/10 CRIMORG 90 ENFOPOL 125 ENFOCUSTOM 36 COMIX 346).

3. Treść podręcznika

Podręcznik jest podzielony na trzy części, które zostały zredagowane w taki sposób, by można było z nich korzystać oddzielnie, w zależności od zamiaru czytelnika.

Pierwsza część podręcznika zawiera **listy kontrolne** zapewniające pragmatyczny zarys możliwości wymiany informacji i powiązanych aspektów praktycznych. Listy te pomogą skierować użytkowników do odpowiedniego punktu kontaktowego do celów wymiany informacji na podstawie wykazów dostępnych systemów i metod w następujących, najważniejszych kontekstach operacyjnych:

- zapobieganie przestępstwom (i imigracji nieuregulowanej) oraz prowadzenie dochodzeń w ich sprawie
- zwalczanie terroryzmu
- utrzymanie porządku publicznego i bezpieczeństwa publicznego.

Po drugie, **ogólny** opis przedstawia zarówno organy krajowe uczestniczące w wymianie informacji, jak i instrumenty wymiany informacji. Podręcznik zawiera odniesienie do kluczowej roli decyzji ramowej Rady 2006/960/WSiSW („szwedzkiej decyzji ramowej”) oraz decyzji Rady 2008/615/WSiSW („decyzja z Prüm”) w szerzej pojmowanej dziedzinie wymiany informacji w UE. Podręcznik nie ogranicza się jednak do tych instrumentów.

Podręcznik został ponadto uzupełniony o zbiór **zestawień informacyjnych dotyczących poszczególnych państw członkowskich**, zawierających **praktyczne informacje na temat punktów kontaktowych** właściwych w przypadku transgranicznej wymiany informacji.

4. Perspektywy

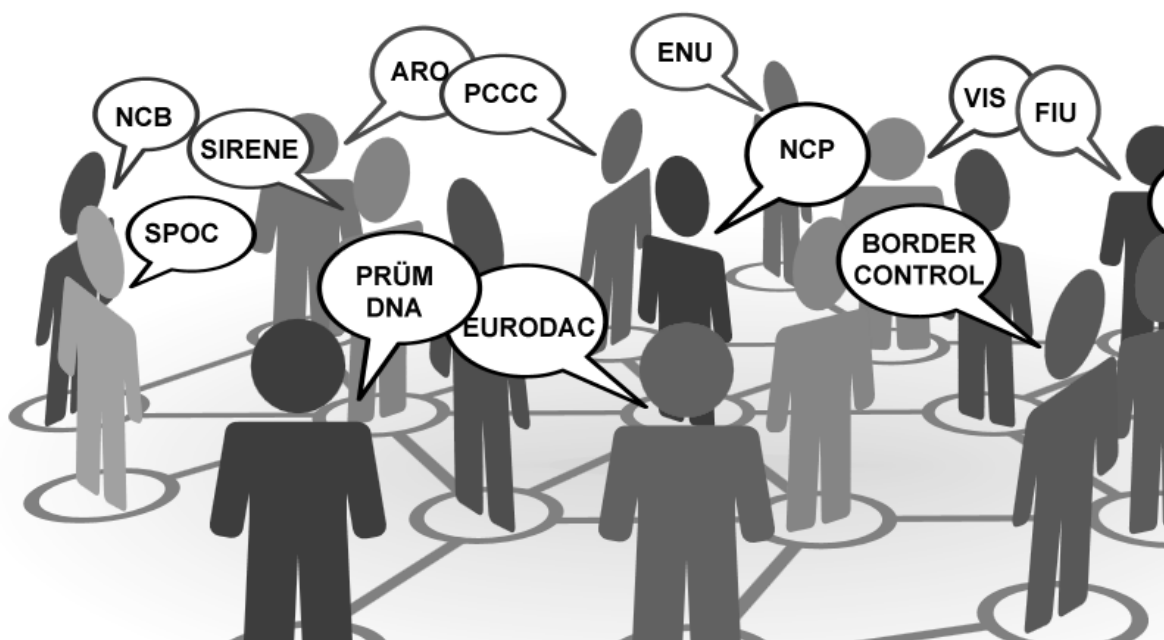
Przygotowanie proponowanego podręcznika było jednym z działań zawartych w 3. wykazie działań służących realizacji strategii w zakresie zarządzania informacjami, a pierwszą wersję podręcznika opracowywano w trakcie prezydencji irlandzkiej, cypryjskiej, greckiej, włoskiej i łotewskiej.

Z myślą o dalszym ułatwieniu stosowania podręcznika dotyczącego wymiany informacji między organami ścigania prezydencja przedkłada delegacjom aktualną, zaktualizowaną wersję i zachęca je do rozpowszechniania podręcznika stosownie do ich potrzeb.



Rada Unii Europejskiej
Sekretariat Generalny
Dyrekcja Generalna ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych
Dyrekcja do Spraw Wewnętrznych
Dział 1C – Współpraca Policyjna i Celna

Podręcznik dotyczący wymiany informacji między organami ścigania



© queidea – Fotolia.com

Spis treści

Wprowadzenie	9
LISTA KONTROLNA A: WYMIANA INFORMACJI DO CELÓW ZAPOBIEGANIA PRZESTĘPSTWOM ORAZ PROWADZENIA DOCHODZEŃ W ICH SPRAWIE	13
LISTA KONTROLNA B: WYMIANA INFORMACJI DO CELÓW ZAPOBIEGANIA PRZESTĘPSTWOM TERRORYSTYCZNYM	20
LISTA KONTROLNA C: WYMIANA INFORMACJI DO CELÓW UTRZYMANIA PORZĄDKU PUBLICZNEGO I BEZPIECZEŃSTWA PUBLICZNEGO	27
CZEŚĆ II – Informacje ogólne	30
1. KANAŁY KOMUNIKACYJNE	31
1.1. SPOC – pojedynczy punkt kontaktowy	31
1.2. Biura SIRENE	35
1.3. Jednostki krajowe Europolu	36
1.4. Krajowe biura Interpolu	37
1.5. Krajowe punkty kontaktowe utworzone na podstawie decyzji z Prüm	38
1.5.1. Krajowe punkty kontaktowe utworzone na podstawie decyzji z Prüm – DNA i odciski palców	38
1.5.2. Krajowe punkty kontaktowe utworzone na podstawie decyzji z Prüm – dane rejestracyjne pojazdów	40
1.5.3. Krajowe punkty kontaktowe utworzone na mocy decyzji z Prüm – zapobieganie terroryzmowi	41
1.5.4. Krajowe punkty kontaktowe utworzone na podstawie decyzji z Prüm – duże imprezy 41	
1.6. Narodowe punkty informacyjne dla piłki nożnej (NFIP)	42
1.6.1. Podręcznik dotyczący meczów piłki nożnej	43
1.7. Centra współpracy policyjno-celnej (PCCC)	44
1.8. Oficerowie łącznikowi	46

1.9.	Biura państw członkowskich ds. odzyskiwania mienia	48
1.10.	Pranie pieniędzy – współpraca między jednostkami analityki finansowej (FIU).....	49
1.11.	Konwencja neapolitańska II.....	51
1.12.	Jednostka do spraw informacji o pasażerach (PIU)	52
1.13.	Wybór kanału – powszechnie stosowane kryteria	55
2.	SYSTEMY INFORMACYJNE	57
2.1.	System informacyjny Schengen drugiej generacji (SIS II).....	57
2.2.	EIS – system informacyjny Europolu	59
2.3.	SIENA – stworzona na potrzeby Europolu aplikacja sieci bezpiecznej wymiany informacji	61
2.4.	System I-24/7 – globalny policyjny system łączności Interpolu	62
2.4.1.	Interpol: brama sieciowa DNA	62
2.4.2.	Baza danych odcisków palców Interpolu.....	62
2.4.3.	Baza zawierająca dane skradzionych lub utraconych dokumentów podróży	63
2.4.4.	Tabela odniesienia Interpolu dotycząca broni palnej.....	63
2.5.	Europejski system przekazywania informacji z rejestrów karnych (ECRIS)	64
2.6.	Wizowy system informacyjny (VIS)	65
2.7.	Eurodac	66
2.8.	CIS – system informacji celnej	69
2.9.	Fałszywe i autentyczne dokumenty online – FADO	70
2.10.	Publiczny rejestr on-line autentycznych dokumentów tożsamości i dokumentów podróży – PRADO	71
2.11.	Przegląd systemów informacyjnych stosowanych do unijnej wymiany informacji	72

3.	PRAWODAWSTWO – KONTEKST PRAWNY, ZASADY I WSKAZÓWKI DOTYCZĄCE PODSTAWOWYCH METOD I SYSTEMÓW ŁĄCZNOŚCI	77
3.0.	Dyrektywa o ochronie danych	77
3.1.	Szwedzka decyzja ramowa	80
3.2.	Schengen – wymiana danych w SIS II i poza tym systemem.....	91
3.3.	Europol.....	94
3.4.	Interpol	96
3.5.	Oficerowie łącznikowi	97
3.6.	Wymiana danych na mocy decyzji z Prüm.....	99
3.7.	Wizowy system informacyjny (VIS)	101
3.8.	Eurodac	102
3.9.	Konwencja neapolitańska II.....	103
3.9.1.	System informacji celnej – CIS	104
3.10.	Biura ds. odzyskiwania mienia (ARO) i CARIN.....	105
3.11.	Jednostki analityki finansowej (FIU).....	106
3.12.	Umowa między UE a USA w sprawie programu śledzenia środków należących do terrorystów (system TFTP)	107
3.13.	Wymiana informacji pochodzących z rejestrów karnych (ECRIS)	109
3.14.	Zatrzymywanie danych telekomunikacyjnych.....	110
3.15.	Dyrektywa w sprawie danych PNR (danych dotyczących przelotu pasażera)	112
3.16.	System danych pasażera przekazywanych przed podróżą (APIS).....	115
3.17.	Przestępstwa lub wykroczenia związane z bezpieczeństwem ruchu drogowego	116

WPROWADZENIE

Cel podręcznika

Transgraniczna współpraca policyjna w obrębie Unii Europejskiej w znacznej mierze opiera się na wymianie informacji. Niniejszy podręcznik ma na celu ułatwienie rutynowej współpracy w tym zakresie. Skierowany jest głównie do pracowników krajowych pojedynczych punktów kontaktowych (SPOC) odpowiedzialnych za zarządzanie przepływem informacji pomiędzy poszczególnymi działami oraz wyznaczonych punktów kontaktowych, zarówno na szczeblu krajowym, jak i międzynarodowym.

Współpracę w dziedzinie egzekwowania prawa w Europie charakteryzuje zwiększenie i przyspieszenie wymiany informacji. Z jednej strony wymianę tę ułatwia nieustanny rozwój technologii informacyjnych i komunikacyjnych. Z drugiej strony istnieje zbyt wiele dostępnych baz danych, zarówno krajowych, jak i międzynarodowych.

Niniejszy podręcznik ma pomóc znaleźć odpowiedni kontakt lub bazę danych w konkretnym kontekście operacyjnym. Przedstawiono w nim również skrótowo odnośne przepisy, jednak bez tracenia z oczu głównego celu, jakim jest ułatwianie transgranicznej wymiany informacji.

Struktura podręcznika

Podręcznik jest podzielony na trzy części:

CZĘŚĆ I – Kontekst operacyjny – zawiera zestaw tabel lub list kontrolnych, w których informacje zawarte w **CZĘŚCI II** i **CZĘŚCI III** połączono z odpowiednią podstawą prawną lub informacjami o punktach kontaktowych. Listy kontrolne podzielone zostały na trzy główne obszary tematyczne:

- **zapobieganie przestępstwom (i imigracji nieuregulowanej) oraz ich zwalczanie – lista kontrolna A**
- **zwalczanie przestępstw terrorystycznych – lista kontrolna B**
- **utrzymywanie porządku publicznego – lista kontrolna C.**

Celem list kontrolnych jest zapewnienie czytelnikowi wskazówek, począwszy od wybranego przezeń odpowiedniego kanału komunikacji lub metody komunikacji w danym kontekście operacyjnym aż do źródła danych kontaktowych lub odpowiednich przepisów ustawowych i wykonawczych, i uregulowań oraz podręczników sprawdzonych rozwiązań.

CZĘŚĆ II – Informacje ogólne – przedstawia strukturę organów ścigania, jeżeli chodzi o różne metody i kanały komunikacji dostępne siłom policyjnym w UE. Część druga została podzielona na trzy obszary tematyczne obejmujące:

- *kanały komunikacyjne (tj. organy uczestniczące w wymianie informacji służących egzekwowaniu prawa)*
- *systemy informacyjne i bazy danych wykorzystywane w transgranicznej wymianie danych*
- *przepisy – kontekst legislacyjny oraz zasady i wskazówki dotyczące podstawowych metod i systemów komunikacji.*

Część III – Zestawienia informacyjne dotyczące poszczególnych państw – w addendum do niniejszej noty; obejmuje zestawienia poświęcone poszczególnym państwom zawierające szczegółowe informacje na temat punktów kontaktowych właściwych w przypadku wszystkich aspektów transgranicznej wymiany informacji, o których mowa w całym dokumencie. Na państwach członkowskich spoczywa obowiązek niezwłocznego powiadamiania Sekretariatu Generalnego Rady o wszelkich zmianach. Regularnie aktualizując zestawienia informacyjne dotyczące poszczególnych państw, zawarte w addendum do podręcznika, państwa członkowskie wypełnią wiele zobowiązań w zakresie powiadamiania nałożonych na nie na mocy różnych instrumentów. Powinno to ułatwić zarządzanie takimi informacjami i ich odszukiwanie w przyszłości.

CZĘŚĆ I – Kontekst operacyjny

LISTA KONTROLNA A: WYMIANA INFORMACJI DO CELÓW ZAPOBIEGANIA PRZESTĘPSTWOM ORAZ PROWADZENIA DOCHODZEŃ W ICH SPRAWIE

System informacyjny	Krajowy punkt dostępu	Podstawa prawna	Podręcznik
System informacyjny Schengen / SIS II	biura Sirene (Supplementary Information Request at the National Entry Bureau)	Dorobek Schengen, o którym mowa w art. 1 ust. 2 decyzji Rady 1999/435/WE z dnia 20 maja 1999 r. Dz.U. L 239 z 22.9.2000, s. 1. Decyzja Rady 2007/533/WSiSW, Dz.U. L 205 z 7.8.2007, s. 63. Rozporządzenie (WE) nr 1986/2006, Dz.U. L 381 z 28.12.2006, s. 1. Rozporządzenie (WE) 1987/2006, Dz.U. L 381 z 28.12.2006, s. 4.	Zmieniona wersja uaktualnionego katalogu zaleceń i wzorcowych rozwiązań co do właściwego stosowania prawnego dorobku Schengen, 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Decyzja wykonawcza Komisji (UE) 2015/219 z dnia 29 stycznia 2015 r. zastępująca załącznik do decyzji wykonawczej 2013/115/UE w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla systemu informacyjnego Schengen drugiej generacji (SIS II) (notyfikowana jako dokument nr C(2015) 326)

Europol / system informacyjny Europolu – katalog EIS Pliki analityczne	Jednostki krajowe	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. 53–114 (mające zastosowanie od 1 maja 2017 r.)	
Interpol – system I-24/7	Krajowe biuro Interpolu (NCB)	Zasady Interpolu dotyczące przetwarzania danych [III/IRPD/GA/2011(2014)] Zasady kontroli informacji i dostępu do danych Interpolu [II.E/RCIA/GA/2004(2009)]	
Profile DNA / decyzja z PRÜM – zautomatyzowane przeszukiwanie wyznaczonych krajowych baz danych	Krajowy punkt kontaktowy 1. krok: zautomatyzowane przeszukiwanie	Decyzja Rady 2008/615/WSiSW, art. 3 i 4, Dz.U. L 210 z 6.8.2008, s. 1.	
	2. krok: dostarczanie kolejnych danych osobowych i innych informacji	Przepisy krajowe Decyzja ramowa Rady 2006/960/WSiSW („szwedzka decyzja ramowa”) Dz.U. L 386 z 29.12.2006, s. 89. Sprostowanie w Dz.U. L 75 z 15.3.2007, s. 26.	

Odciski palców / zautomatyzowane przeszukiwanie krajowych automatycznych systemów identyfikacji daktyloskopijnej (AFIS) na mocy decyzji z PRÜM	Krajowy punkt kontaktowy 1. krok: zautomatyzowane przeszukiwanie	Decyzja Rady 2008/615/WSiSW, art. 9, Dz.U. L 210 z 6.8.2008, s. 1.	
	2. krok: dostarczanie kolejnych danych osobowych i innych informacji	Przepisy krajowe Decyzja ramowa Rady 2006/960/WSiSW („szwedzka decyzja ramowa”)	
Dane rejestracyjne pojazdów / decyzja z PRÜM – zautomatyzowane przeszukiwanie baz danych rejestracyjnych pojazdów	Krajowy punkt kontaktowy – wnioski przychodzące	Decyzja Rady 2008/615/WSiSW, art. 12, Dz.U. L 210 z 6.8.2008, s. 1.	
	– wnioski wychodzące	j.w.	
Dane dotyczące przelotu pasażera (PNR) Termin wdrożenia: 25 maja 2018 r.	Jednostka do spraw informacji o pasażerach (PIU)	Dyrektywa Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania Dz.U. L 119 z 4.5.2016, s. 132.	

Wizowy system informacyjny / VIS	Krajowe centralne punkty dostępu	Decyzja Rady 2004/512/WE, Dz.U. L 213 z 15.6.2004, s. 5. Decyzja Rady 2008/633/WSiSW, Dz.U. L 218 z 13.8.2008, s. 126. Wykaz właściwych organów, których odpowiednio upoważniony personel ma dostęp pozwalający wprowadzać, modyfikować, usuwać lub przeglądać dane w Wizowym Systemie Informacyjnym (VIS) (2016/C 187/04), Dz.U. C 187 z 26.5.2016, s. 4.	
----------------------------------	----------------------------------	---	--

Eurodac	Właściwe organy krajowe	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona) Dz.U. L 180 z 29.6.2013, s. 1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca Dz.U. L 180 z 29.6.2013, s. 31.	
---------	-------------------------	---	--

CIS – system informacji celnej	Krajowe punkty dostępu	Decyzja Rady 2009/917/WSiSW w sprawie stosowania technologii informatycznej do potrzeb celnych Dz.U. L 323 z 10.12.2009, s. 20.	
Europejski system przekazywania informacji z rejestrów karnych / ECRIS	Krajowy organ centralny	Decyzja Rady 2009/316/WSiSW, Dz.U. L 93 z 7.4.2009, s. 33.	ECRIS – Niewiążący podręcznik dla użytkowników systemu ECRIS Dostępny w formacie elektronicznym na stronie CIRCABC: https://circabc.europa.eu
Międzyagencyjna Sieć Odzyskiwania Mienia Camden (CARIN)	Biuro ds. odzyskiwania mienia	Decyzja Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotycząca współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem Dz.U. L 332 z 18.12.2007, s. 103.	Podręcznik dobrych praktyk w zwalczaniu przestępstw finansowych: zbiór wzorcowych przykładów dobrze rozwiniętych systemów istniejących w państwach członkowskich służących zwalczaniu przestępstw finansowych 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37

FIU.NET (Sieć Jednostek Analityki Finansowej)	Jednostki analityki finansowej (FIU)	Decyzja Rady 2000/642/WSiSW z dnia 17 października 2000 r. dotycząca uzgodnień w sprawie współpracy pomiędzy jednostkami wywiadu finansowego państw członkowskich w odniesieniu do wymiany informacji Dz.U. L 271 z 24.10.2000, s. 4. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 658/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE Dz.U. L 141 z 5.6.2015, s. 73.	Podręcznik dobrych praktyk w zwalczaniu przestępstw finansowych: zbiór wzorcowych przykładów dobrze rozwiniętych systemów istniejących w państwach członkowskich służących zwalczaniu przestępstw finansowych 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37
---	--------------------------------------	---	--

LISTA KONTROLNA B: WYMIANA INFORMACJI DO CELÓW ZAPOBIEGANIA PRZESTĘPSTWOM TERRORYSTYCZNYM

System informacyjny	Krajowy punkt dostępu	Podstawa prawna	Podręcznik
System informacyjny Schengen / SIS II	biura Sirene (Supplementary Information Request at the National Entry Bureau)	Dorobek Schengen, o którym mowa w art. 1 ust. 2 decyzji Rady 1999/435/WE z dnia 20 maja 1999 r. Dz.U. L 239 z 22.9.2000, s. 1. Decyzja Rady 2007/533/WSiSW, Dz.U. L 205 z 7.8.2007, s. 63. Rozporządzenie (WE) nr 1986/2006, Dz.U. L 381 z 28.12.2006, s. 1. Rozporządzenie (WE) 1987/2006, Dz.U. L 381 z 28.12.2006, s. 4.	Zmieniona wersja uaktualnionego katalogu zaleceń i wzorcowych rozwiązań co do właściwego stosowania prawnego dorobku Schengen, 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Decyzja wykonawcza Komisji (UE) 2015/219 z dnia 29 stycznia 2015 r. zastępująca załącznik do decyzji wykonawczej 2013/115/UE w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla systemu informacyjnego Schengen drugiej generacji (SIS II) (notyfikowana jako dokument nr C(2015) 326)

Europol / system informacyjny Europolu – katalog EIS Pliki analityczne	Jednostki krajowe	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. 53–114 (mające zastosowanie od 1 maja 2017 r.)	
Interpol – system I-24/7	Krajowe biuro Interpolu (NCB)	Zasady Interpolu dotyczące przetwarzania danych [III/IRPD/GA/2011(2014)] Zasady kontroli informacji i dostępu do danych Interpolu [II.E/RCIA/GA/2004(2009)]	
Profile DNA / decyzja z PRÜM – zautomatyzowane przeszukiwanie wyznaczonych krajowych baz danych	Krajowy punkt kontaktowy 1. krok: zautomatyzowane przeszukiwanie	Decyzja Rady 2008/615/WSiSW, art. 3 i 4, Dz.U. L 210 z 6.8.2008, s. 1.	
	2. krok: dostarczanie kolejnych danych osobowych i innych informacji	Przepisy krajowe Decyzja ramowa Rady 2006/960/WSiSW („szwedzka decyzja ramowa”) Dz.U. L 386 z 29.12.2006, s. 89. Sprostowanie w Dz.U. L 75 z 15.3.2007, s. 26.	

Odciski palców / zautomatyzowane przeszukiwanie krajowych automatycznych systemów identyfikacji daktyloskopijnej (AFIS) na mocy decyzji z PRÜM	Krajowy punkt kontaktowy 1. krok: zautomatyzowane przeszukiwanie	Decyzja Rady 2008/615/WSiSW, art. 9, Dz.U. L 210 z 6.8.2008, s. 1.	
	2. krok: dostarczanie kolejnych danych osobowych i innych informacji	Przepisy krajowe Decyzja ramowa Rady 2006/960/WSiSW („szwedzka decyzja ramowa”)	
Dane rejestracyjne pojazdów / decyzja z PRÜM – zautomatyzowane przeszukiwanie baz danych rejestracyjnych pojazdów	Krajowy punkt kontaktowy – wnioski przychodzące	Decyzja Rady 2008/615/WSiSW, art. 12, Dz.U. L 210 z 6.8.2008, s. 1.	
	– wnioski wychodzące	j.w.	
Profile DNA / decyzja z PRÜM – zautomatyzowane przeszukiwanie wyznaczonych krajowych baz danych	Krajowy punkt kontaktowy 1. krok: zautomatyzowane przeszukiwanie	Decyzja Rady 2008/615/WSiSW, art. 3 i 4, Dz.U. L 210 z 6.8.2008, s. 1.	<i>Podręcznik wdrażania – wymiana danych DNA</i> 7148/15 DAPIX 40 CRIMORG 25 ENFOPOL 61
Sieć PRÜM do przekazywania danych osobowych i określonych informacji służących zapobieganiu przestępstwom terrorystycznym	Krajowy punkt kontaktowy ds. walki z terroryzmem utworzony na podstawie decyzji z Prüm	Decyzja Rady 2008/615/WSiSW, art. 16, Dz.U. L 210 z 6.8.2008, s. 1.	

Dane dotyczące przelotu pasażera (PNR) Termin wdrożenia: 25 maja 2018 r.	Jednostka do spraw informacji o pasażerach (PIU)	Dyrektywa Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania Dz.U. L 119 z 4.5.2016, s. 132.	
Wizowy system informacyjny / VIS	Krajowe centralne punkty dostępu	Decyzja Rady 2004/512/WE, Dz.U. L 213 z 15.6.2004, s. 5. Decyzja Rady 2008/633/WSiSW, Dz.U. L 218 z 13.8.2008, s. 126. Wykaz właściwych organów, których odpowiednio upoważniony personel ma dostęp pozwalający wprowadzać, modyfikować, usuwać lub przeglądać dane w Wizowym Systemie Informacyjnym (VIS) (2016/C 187/04), Dz.U. C 187 z 26.5.2016, s. 4.	

Eurodac	Właściwe organy krajowe	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona) Dz.U. L 180 z 29.6.2013, s. 1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca Dz.U. L 180 z 29.6.2013, s. 31.	
---------	-------------------------	---	--

Europejski system przekazywania informacji z rejestrów karnych / ECRIS	Krajowy organ centralny	Decyzja Rady 2009/316/WSiSW, Dz.U. L 93 z 7.4.2009, s. 33.	ECRIS – Niewiążący podręcznik dla użytkowników systemu ECRIS Dostępny w formacie elektronicznym na stronie CIRCABC: https://circabc.europa.eu
Międzyagencyjna Sieć Odzyskiwania Mienia Camden (CARIN)	Biuro ds. odzyskiwania mienia	Decyzja Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotycząca współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem Dz.U. L 332 z 18.12.2007, s. 103.	

FIU.NET (Sieć Jednostek Analityki Finansowej)	Jednostki analityki finansowej (FIU)	Decyzja Rady 2000/642/WSiSW z dnia 17 października 2000 r. dotycząca uzgodnień w sprawie współpracy pomiędzy jednostkami wywiadu finansowego państw członkowskich w odniesieniu do wymiany informacji Dz.U. L 271 z 24.10.2000, s. 4. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 658/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE Dz.U. L 141/73 z 5.6.2015.	
---	--------------------------------------	---	--

LISTA KONTROLNA C: WYMIANA INFORMACJI DO CELÓW UTRZYMANIA PORZĄDKU PUBLICZNEGO I BEZPIECZEŃSTWA PUBLICZNEGO

System informacyjny	Krajowy punkt dostępu	Podstawa prawna	
Sieć stałych punktów kontaktowych ds. porządku publicznego	Krajowe punkty kontaktowe	Wspólne działanie 97/339/WSiSW z dnia 26 maja 1997 r. przyjęte przez Radę na podstawie art. K.3 Traktatu o Unii Europejskiej, dotyczące współpracy w zakresie porządku publicznego i bezpieczeństwa, art. 3 lit. b), Dz.U. L 147 z 5.6.1997, s. 1.	
Sieć PRÜM do przekazywania danych nieosobowych i osobowych do celów prewencji kryminalnej oraz ochrony porządku i bezpieczeństwa publicznego podczas dużych imprez o wymiarze transgranicznym	Krajowy punkt kontaktowy utworzony na podstawie decyzji z Prüm / duże imprezy	Decyzja Rady 2008/615/WSiSW, art. 15, Dz.U. L 210 z 6.8.2008, s. 1. Przepisy krajowe	

Sieć narodowych punktów informacyjnych dla piłki nożnej	Narodowe punkty informacyjne dla piłki nożnej / NFIP	Decyzja Rady 2002/348/WSiSW z dnia 25 kwietnia 2002 r. dotycząca bezpieczeństwa w związku z meczami piłki nożnej o charakterze międzynarodowym, Dz.U. L 121 z 8.5.2002, s. 1. Decyzja Rady 2007/412/WSiSW z dnia 12 czerwca 2007 r. zmieniająca decyzję 2002/348/WSiSW dotyczącą bezpieczeństwa w związku z meczami piłki nożnej o charakterze międzynarodowym, Dz.U. L 155 z 15.6.2007, s. 76.	Zalecenie Rady z dnia 6 grudnia 2007 r. w sprawie Podręcznika współpracy podczas ważnych imprez międzynarodowych przeznaczonego dla policji i organów bezpieczeństwa, Dz.U. C 314 z 22.12.2007, s. 4. Rezolucja Rady z dnia 3 czerwca 2010 r. w sprawie zaktualizowanego podręcznika z zaleceniami w zakresie międzynarodowej współpracy policyjnej oraz w zakresie działań prewencyjnych i kontrolnych związanych z aktami przemocy i zakłóceniami porządku podczas międzynarodowych meczów piłki nożnej, które dotyczą co najmniej jednego państwa członkowskiego Dz.U. C 165 z 24.6.2010, s. 1.
---	--	---	--

Europejska sieć ochrony osób publicznych	Krajowe punkty dostępu	Decyzja Rady 2009/796/WSiSW z dnia 4 czerwca 2009 r. zmieniająca decyzję 2002/956/WSiSW ustanawiającą europejską sieć ochrony osób publicznych, Dz.U. L 283 z 30.10.2009, s. 62.	Podręcznik europejskiej sieci ochrony osób publicznych 10478/13 ENFOPOL 173
Centra współpracy policyjno-celnej	PCCC	Umowy dwustronne	

CZEŚĆ II – INFORMACJE OGÓLNE

1. KANAŁY KOMUNIKACYJNE¹

1.1. SPOC – pojedynczy punkt kontaktowy

Liczne krajowe punkty kontaktowe

Państwa członkowskie, zarówno jako państwa, do których wystąpiono z wnioskiem, jak i jako państwa występujące z wnioskiem, radzą sobie z rosnącym transgranicznym przepływem informacji poprzez poprawę efektywności struktur operacyjnych i sieci – zarówno na szczeblu krajowym, jak i europejskim. Wiele instrumentów prawnych UE dotyczących współpracy transgranicznej w zakresie egzekwowania prawa wymaga ustanowienia specjalnych właściwych władz / organów / biur lub krajowych punktów kontaktowych. Organy policji, organy celne lub inne właściwe organy upoważnione na mocy prawa krajowego muszą wymieniać informacje za pośrednictwem tych wyznaczonych krajowych punktów kontaktowych, którymi w danym państwie członkowskim mogą być różne wydziały policji lub nawet różne ministerstwa. Aby zapewnić pełny obraz, w części III niniejszego dokumentu umieszczono – regularnie publikowane i aktualizowane przez SGR – wykazy konkretnych krajowych punktów kontaktowych ds. wymiany informacji na szczeblu UE w dziedzinie wymiany danych związanych z egzekwowaniem prawa.

Zasada dostępności – szwedzka decyzja ramowa

Wymiana informacji służących egzekwowaniu prawa i danych wywiadowczych o znaczeniu transgranicznym powinna przebiegać na warunkach, które wynikają z „zasady dostępności” wdrażanej na mocy szwedzkiej decyzji ramowej. Oznacza to, że:

- funkcjonariusz organów ścigania w jednym państwie członkowskim, który potrzebuje informacji w celu wykonywania swoich obowiązków, może je uzyskać od drugiego państwa członkowskiego oraz że
- organy ścigania w państwie członkowskim, które posiada te informacje, udostępniają je w zadeklarowanym celu, z uwzględnieniem potrzeb dochodzeń właśnie prowadzonych w tym państwie członkowskim, oraz że
- kiedy informacje policyjne są dostępne w państwie członkowskim, można je przekazać za granicę na tych samych warunkach jak warunki, które regulują wymianę informacji na szczeblu krajowym, co oznacza, że przepisy stosowane w przypadku przekazywania za granicę **nie są bardziej rygorystyczne** niż przepisy stosowane do wymiany danych na poziomie krajowym („zasada równego dostępu”).

¹ Organy krajowe uczestniczące w wymianie informacji służących egzekwowaniu prawa.

Pojedynczy punkt kontaktowy (SPOC)

Połączenie rygorystycznych wymogów szwedzkiej decyzji ramowej i faktu, że istnieją różne krajowe strategie zarządzania różnymi inicjatywami w zakresie wymiany informacji, wymaga prostego i jednolitego podejścia na szczeblu państw członkowskich w celu zapewnienia, by wszystkie wnioski o udzielenie informacji między organami ścigania w UE były rozpatrywane skutecznie i wydajnie.

W konkluzjach Rady na temat europejskiego modelu wymiany informacji (EIXM)², przyjętych w czerwcu 2013 r., uznano potencjał pojedynczego punktu kontaktowego ds. wymiany informacji w każdym państwie członkowskim, jeśli chodzi o usprawnienie tego procesu w coraz bardziej złożonym otoczeniu prawnym i operacyjnym.

Polityka dokonywania wymiany jak największej liczby informacji za pośrednictwem pojedynczego punktu kontaktowego została wdrożona przez prawie wszystkie państwa członkowskie, chociaż rozumienie tego, czym powinien się charakteryzować taki punkt, różni się w poszczególnych państwach członkowskich. W wytycznych dotyczących pojedynczych punktów kontaktowych³ wskazano, w jaki sposób mogą być zorganizowane takie punkty, by zmaksymalizować wykorzystanie zasobów, unikać powielania zadań i sprawić, by współpraca z innymi państwami członkowskimi była skuteczniejsza, korzystniejsza i bardziej przejrzysta.

Państwa członkowskie powinny wybrać z tych wytycznych rozwiązanie odpowiednie do ich sytuacji, kierując się wspólnym i uzgodnionym celem, jakim jest zacieśnienie współpracy międzynarodowej; powinny też rozważyć stosowne sposoby informowania innych państw członkowskich o wybranym rozwiązaniu, z myślą o wymianie optymalnych rozwiązań.

² Konkluzje Rady w następstwie komunikatu Komisji na temat europejskiego modelu wymiany informacji (EIXM), 9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146.

³ „Projekt wytycznych dla pojedynczych punktów kontaktowych (SPOC) dotyczących międzynarodowej wymiany informacji między organami ścigania“, 10492/14 DAPIX 75 ENFOPOL 157 oraz 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1.

Najlepiej, by SPOC:

- miał dostęp do jak najliczniejszych odnośnych krajowych, europejskich i międzynarodowych baz danych organów ścigania, aby sprawnie zarządzać bezpośrednią wymianą informacji między właściwymi organami krajowymi;
- obejmował krajowe jednostki Sirene, Europolu i Interpolu;
- obejmował punkt kontaktowy dla oficerów łącznikowych, punkty kontaktowe wyznaczone na mocy szwedzkiej decyzji ramowej i decyzji z Prüm, oraz – w stosownym przypadku – punkty kontaktowe dla biur regionalnych i dwustronnych;
- działał w bezpiecznym otoczeniu oraz dysponował wystarczającymi i odpowiednimi zasobami kadrowymi, w tym zapewniał usługi tłumaczenia ustnego i pisemnego, co umożliwi mu funkcjonowanie całodobowo. W możliwie największym zakresie wszyscy pracownicy powinni być przeszkoleni oraz wyposażeni/upoważnieni do wykonywania wszelkiego rodzaju zadań w obrębie pojedynczego punktu kontaktowego. Jeżeli nie jest to możliwe, należy zadbać o to, by oficerowie dyżurni dostępni 24 godziny na dobę przez 7 dni w tygodniu byli w stanie wykonywać wszystkie zadania;
- był strukturą wieloagencyjną, w której skład wchodzi personel pochodzący z / należący do różnych służb lub ministerstw, w tym policji kryminalnej, straży granicznej, organów celnych i sądowych.

Typowa struktura biura krajowego SPOC

Centralna jednostka ds. policyjnej współpracy operacyjnej, platforma wymiany informacji

*Punkt taki jest jednostką **międzyrządową**, złożoną z 67 funkcjonariuszy policji, żandarmerii i służb celnych. W tych samych pomieszczeniach sędziowie biura współpracy międzynarodowej w sprawach karnych (B.E.P.I.) Ministerstwa Sprawiedliwości zapewniają także podstawową usługę polegającą na zatwierdzaniu francuskich wniosków o wydanie europejskiego nakazu aresztowania i rejestracji w krajowych aktach osób poszukiwanych wniosków o aresztowanie i czerwonych listów gończych Interpolu.*

*Aby zapewnić niezbędny **przekrojowy charakter** trzech kanałów współpracy, w sierpniu 2004 r. w obrębie centralnej jednostki policyjnej współpracy operacyjnej wyznaczono centralny punkt kontaktowy. Głównym zadaniem osoby pełniącej tę funkcję jest wspieranie francuskich organów ścigania w wyborze najlepszego narzędzia współpracy policyjnej w zależności od charakteru i złożoności prowadzonych dochodzeń. Sprawdza ona, czy wniosek jest zgodny z prawem, przeprowadza pierwsze kontrole krzyżowe i kieruje wniosek do najwłaściwszego kanału współpracy z uwzględnieniem, biorąc pod uwagę zapytanie prowadzących dochodzenie. Do wyłącznych kompetencji SIRENE we Francji należą jedynie wnioski dotyczące wpisów Schengen.*

*Po skutecznym połączeniu zasobów punkt ten przyjmuje, pracując **24 godziny na dobę**, mimo ograniczonej liczby personelu, **prawie 350 000 wiadomości rocznie** w ramach pojedynczej bezpiecznej platformy.*

Wielokanałowa jurysdykcja punktu umożliwia mu zapewnienie Francji reprezentacji w europejskich grupach (SIS / VIS, SIS/SIRENE, szefowie jednostek krajowych Europolu) czy grupach Interpolu (posiedzenie oficerów łącznikowych Interpolu, grupa ds. listów gończych) oraz zapewnia stosowny operacyjny punkt widzenia jednostce ds. informacji odpowiedzialnej we Francji za monitorowanie organów zarządczych Interpolu i Europolu.

1.2. Biura SIRENE

Biura Sirene mają kluczowe znaczenie dla operacji i wymiany informacji w zakresie SIS. W każdym z państw członkowskich ustanowione zostały stałe biura Sirene (ds. wniosków o informacje uzupełniające na wejściach krajowych – **Supplementary Information Request at the National Entry**), które w ramach dorobku Schengen⁴ funkcjonują jako wyznaczone organy, na których spoczywa główna odpowiedzialność za krajowe moduły systemu informacyjnego Schengen (SIS II). Są one punktem kontaktowym dla biur SIRENE innych umawiających się stron i współpracują z krajowymi organami i agencjami. SIS II jest systemem trafieniowym (figuruje / nie figuruje) opierającym się na wyszukiwaniach. Działając w systemie ciągłym (24/7), biura wymieniają dane dotyczące wpisów w SIS II⁵, czyli zestawów danych, które umożliwiają organom zidentyfikowanie osób lub przedmiotów z myślą o podjęciu stosownych działań.

„Informacje uzupełniające” to informacje, które nie są przechowywane w SIS II, ale są związane z wpisami w SIS II, i które wymienia się – dwustronnie lub wielostronnie – w postaci formularzy:

- (i) w celu umożliwienia państwom członkowskim wzajemnej konsultacji lub wzajemnego informowania się podczas dokonywania wpisu;
- (ii) w celu umożliwienia podjęcia odpowiednich działań po uzyskaniu trafienia;
- (iii) w przypadku niemożności podjęcia wymaganego działania;
- (iv) w kwestiach dotyczących jakości danych SIS II;
- (v) w kwestiach dotyczących zgodności i priorytetu wpisów;
- (vi) w kwestiach związanych z prawami dostępu.

⁴ Zob. konwencja wykonawcza do układu z Schengen, Dz.U. L 239 z 22.9.2000.

⁵ Zob. 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.

Informacje są wymieniane zgodnie z wytycznymi zawartymi w podręczniku SIRENE⁶ za pośrednictwem infrastruktury łączności⁷. W porównaniu ze swoim poprzednikiem SIS II⁸ ma zaawansowane funkcje, takie jak możliwość wprowadzania odcisków palców i zdjęć, nowych rodzajów przedmiotów (skradzione statki powietrzne, łodzie, kontenery, środki płatnicze) oraz możliwość wprowadzania przez właściciela wpisu odsyłaczy do innych wpisów. SIS II zawiera kopie europejskiego nakazu aresztowania dołączone bezpośrednio do wpisów dotyczących osób.

Biura SIRENE ułatwiają współpracę w kwestiach dotyczących policji i mogą również odgrywać rolę w wymianie informacji poza zakresem SIS II zgodnie z przepisami poprzednio objętymi art. 39 i 46 konwencji z Schengen, które zostały zastąpione **szwedzką decyzją ramową**. Zgodnie z art. 12 ust. 1 szwedzkiej decyzji ramowej postanowienia art. 39 ust. 1, 2 i 3 oraz art. 46 konwencji wykonawczej do układu z Schengen, w zakresie, w jakim odnoszą się one do przewidzianej w tej decyzji ramowej wymiany informacji i danych wywiadowczych do celów prowadzenia dochodzeń lub operacji wywiadowczych w sprawie przestępstw, zastępuje się przepisami decyzji ramowej.

1.3. Jednostki krajowe Europolu

Każde państwo członkowskie dysponuje wyznaczoną krajową jednostką Europolu, która jest organem pośredniczącym w kontaktach między Europolem a właściwymi organami krajowymi. Oficerowie łącznikowi jednostek krajowych Europolu oddelegowani do Europolu powinni zapewniać całodobowy kontakt między siedzibą Europolu w Hadze a jednostkami krajowymi Europolu w 28 państwach członkowskich. W ramach Europolu pracują także oficerowie łącznikowi z dziesięciu państw i organizacji spoza UE. Sieć ma do dyspozycji bezpieczne kanały informacyjne zapewnione przez Europol.

⁶ Decyzja wykonawcza Komisji z dnia 26 lutego 2013 r. w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla systemu informacyjnego Schengen drugiej generacji (SIS II) (notyfikowana jako dokument nr C(2013) 1043), Dz.U. L 71 z 14.3.2013, s. 1.

⁷ Z uwagi na zamknięcie sieci poczty elektronicznej Sisnet biura Sirene mogą obecnie korzystać z poczty elektronicznej sTESTA. Wymiana innych informacji może odbywać się poprzez sieć sTESTA, SIENA lub kanały komunikacyjne Interpolu działające w systemie I-24/7.

⁸ Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie oceny Systemu Informacyjnego Schengen drugiej generacji (SIS II) zgodnie z art. 24 ust. 5, art. 43 ust. 3 i art. 50 ust. 5 rozporządzenia (WE) nr 1987/2006 i art. 59 ust. 3 i art. 66 ust. 5 decyzji 2007/533/WSiSW; 15810/16 SIRIS 175 COMIX 860.

Europol⁹ wspiera organy ścigania państw członkowskich w zapobieganiu przestępczości zorganizowanej, poważnej przestępczości międzynarodowej i aktom terroryzmu, gdy obejmują one co najmniej dwa państwa członkowskie, oraz w zwalczaniu tych zjawisk. Aby móc gromadzić, przechowywać, przetwarzać i analizować dane osobowe oraz by wymieniać informacje i dane wywiadowcze, Europol musi korzystać z danych otrzymanych od państw członkowskich. Rozporządzenie Rady w sprawie Europolu określa różne zadania informacyjne oraz zasady dotyczące wykorzystywania danych i ich wymiany ze stronami trzecimi w ramach solidnego systemu ochrony danych i bezpieczeństwa.

1.4. Krajowe biura Interpolu

Krajowe biura Interpolu w komendach głównych policji odgrywają kluczową rolę przy przetwarzaniu w systemie informacyjnym Interpolu danych przekazywanych przez te państwa. Biura te są upoważnione do bezpośredniego dostępu do systemu, co obejmuje:

- rejestrowanie, aktualizowanie i usuwanie danych bezpośrednio w policyjnych bazach danych, a także tworzenie powiązań między danymi;
- bezpośrednie przeglądanie tych baz danych;
- korzystanie z listów gończych i ogłoszeń Interpolu do przekazywania wniosków o współpracę i wpisów międzynarodowych.

Krajowe biura Interpolu mogą szybko przeszukiwać i prowadzić kontrole krzyżowe danych, dysponując w systemie ciągłym (24/7) bezpośrednim dostępem do baz danych zawierających informacje na temat osób podejrzanych o działalność terrorystyczną, osób poszukiwanych, odcisków palców, profili DNA, zagubionych lub skradzionych dokumentów podróży, skradzionych pojazdów silnikowych, skradzionych dzieł sztuki itp.

⁹ 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. 53–114 (mające zastosowanie od 1 maja 2017 r.)

W miarę możliwości krajowe biura Interpolu powinny umożliwić organom dochodzeniowym ich państw uczestniczącym w międzynarodowej współpracy policyjnej dostęp do systemu informacji Interpolu. Krajowe biura Interpolu kontrolują poziom dostępu do usług Interpolu, jakim dysponują inni uprawnieni użytkownicy z ich państw, i mogą zwracać się o informacje o zapytaniach, jakie do ich krajowych baz danych kierują inne państwa.

1.5. Krajowe punkty kontaktowe utworzone na podstawie decyzji z Prüm

Decyzje z Prüm¹⁰ otworzyły nowy transgraniczny wymiar zwalczania przestępczości poprzez zapewnienie wzajemnego transgranicznego dostępu online do wyznaczonych krajowych baz danych DNA, automatycznych systemów identyfikacji daktyloskopijnej (AFIS) oraz baz danych rejestracyjnych pojazdów. W każdym uczestniczącym państwie członkowskim wyznaczono dla każdego rodzaju wymiany specjalny krajowy punkt kontaktowy, który odpowiada za dostarczanie danych¹¹. Ochrona danych i dostosowane do potrzeb przepisy dotyczące bezpieczeństwa danych w szczególności uwzględniają wyjątkowy charakter dostępu online do tych baz danych. Dostarczanie danych osobowych wymaga odpowiedniego poziomu ochrony i bezpieczeństwa danych, wzajemnie sprawdzonego i uzgodnionego przez państwa członkowskie przed rozpoczęciem wymiany danych.

1.5.1. Krajowe punkty kontaktowe utworzone na podstawie decyzji z Prüm – DNA i odciski palców

W przypadku danych dotyczących DNA i odcisków palców automatyzowane porównywanie referencyjnych danych biometrycznych opiera się na systemie trafieniowym („figuruje/nie figuruje”). Dane referencyjne nie pozwalają na natychmiastową identyfikację podmiotu danych. W przypadku trafienia krajowy punkt kontaktowy państwa członkowskiego przeszukującego dane może zatem zwrócić się o dodatkowe szczegółowe dane osobowe. O dostarczenie tego rodzaju dodatkowych danych należy wystąpić w trybie procedur wzajemnej pomocy, także tych przyjętych na mocy szwedzkiej decyzji ramowej. Dostarczanie podlega prawu krajowemu, w tym przepisom o pomocy prawnej, państwa członkowskiego, do którego wystąpiono z wnioskiem.

¹⁰ Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz.U. L 210 z 6.8.2008, s. 1; Decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. w sprawie wdrożenia decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.U. L 210 z 6.8.2008, s. 12)

¹¹ 5010/15 JAI 1 DAPIX 1 ENFOPOL 1 CRIMORG 1.

1.5.1.1. Przewodnik dobrych praktyk w zakresie przeszukiwania odcisków palców

W przypadku stosowania zautomatyzowanego narzędzia Prüm służącego do przeszukiwania baz odcisków palców występujące z wnioskiem państwo członkowskie powinno postępować zgodnie z zaleceniami zawartymi w dokumencie *Dobre praktyki w zakresie przeglądania baz danych państw członkowskich* (dok. 14885/1/08 REV1). W dokumencie tym uznano ograniczone możliwości przeszukiwania **baz danych daktyloskopijnych** oraz zalecono propagowanie na poziomie operacyjnym następujących praktyk:

- Ewentualne skorzystanie z będących w dyspozycji państw członkowskich baz danych daktyloskopijnych oraz kolejność przeprowadzania takich poszukiwań i ich powtarzania to czynności dochodzeniowe podejmowane oddzielnie dla każdego przypadku i nie należy o nich decydować z wyprzedzeniem.
- Bazy danych daktyloskopijnych innych państw członkowskich zasadniczo nie powinny być przeszukiwane, do czasu gdy państwo występujące z wnioskiem przeszuka własną(-e) bazę(-y) danych daktyloskopijnych.
- Podejmując decyzję o przeszukaniu jednej lub kilku baz danych państw członkowskich, należy uwzględniać w szczególności:
 - powagę sprawy;
 - lub istniejące wątki dochodzenia, w szczególności informacje wskazujące na dane państwo członkowskie lub grupę państw członkowskich;
 - lub szczególne wymogi dochodzenia.
- Wyszukiwania ogólne powinno się prowadzić jedynie w przypadku, gdy wyczerpano dobre praktyki opisane w punktach 1–3.

Przykłady zautomatyzowanej wymiany danych na mocy decyzji Rady dotyczących konwencji z Prüm

W 2011 r., w trakcie dochodzenia w sprawie zabójstwa, do czeskiej krajowej bazy danych DNA wprowadzono informację o materiale genetycznym. Dochodzenie było prowadzone przeciwko podejrzanemu, który zbiegł za granicę. Materiał genetyczny uzyskano z niedopałka papierosa znalezionej w popielniczce w mieszkaniu, w którym przestępstwo zostało popełnione. Po przeszukaniu w 2014 r. austriackiej bazy danych DNA stwierdzono, że dane dotyczące tego samego profilu były już przetwarzane w Austrii. Pojedyncze punkty kontaktowe obu państw wymieniły kolejne dane osobowe w ramach współpracy policyjnej. Następnie skontaktowano się z austriackim departamentem ds. wymiaru sprawiedliwości w sprawach karnych i za pośrednictwem procedur pomocy prawnej w sprawach karnych poproszono o przekazanie podejrzanego do Republiki Czeskiej, gdzie prowadzono postępowanie karne.

W 2005 r., w trakcie dochodzenia w sprawie rozboju, do czeskiej krajowej bazy danych DNA wprowadzono informację o profilu DNA. Podejrzanego wskazano w 2014 r. po przeszukaniu austriackiej bazy danych DNA. Poproszono stronę austriacką o dostarczenie za pośrednictwem pojedynczych punktów kontaktowych aktualnej fotografii i innych danych osobowych.

1.5.2. Krajowe punkty kontaktowe utworzone na podstawie decyzji z Prüm – dane rejestracyjne pojazdów

Jeżeli chodzi o dane rejestracyjne pojazdów, dane można przeszukiwać według pełnego numeru podwozia w jednym lub we wszystkich uczestniczących państwach członkowskich bądź według pełnego numeru rejestracyjnego w jednym konkretnym państwie członkowskim. Informacje wymienia się poprzez krajowe punkty kontaktowe wyznaczone do obsługi zarówno wniosków przychodzących, jak i wychodzących. Państwa członkowskie przyznają sobie nawzajem dostęp online do krajowych danych rejestracyjnych pojazdów w odniesieniu do:

- a) danych właścicieli lub użytkowników; oraz
- b) danych pojazdu.

Państwa członkowskie wykorzystują jedną z wersji oprogramowania europejskiego systemu informacji o pojazdach i prawach jazdy (EUCARIS) specjalnie zaprojektowaną do celów Prüm do przeprowadzania takich przeszukań. Przeszukiwanie danych rejestracyjnych pojazdów różni się od przeszukiwania danych dotyczących DNA i odcisków palców, gdyż w przypadku trafienia otrzymuje się zarówno dane osobowe, jak i referencyjne. Jak w przypadku innych zautomatyzowanych wyszukiwań uznaje się, że dostarczanie danych osobowych podlega odpowiedniemu poziomowi ochrony danych stosowanemu przez państwo członkowskie je otrzymujące.

1.5.3. Krajowe punkty kontaktowe utworzone na mocy decyzji z Prüm – zapobieganie terroryzmowi

Na żądanie lub z własnej inicjatywy wyznaczone krajowe punkty kontaktowe mogą wymieniać informacje na temat osób podejrzanych o popełnienie przestępstw terrorystycznych. Dane te obejmują nazwisko, imiona, datę i miejsce urodzenia podejrzanego oraz opis okoliczności dających podstawy do przypuszczenia, że podmiot danych popełni przestępstwo związane z działalnością terrorystyczną.

Dostarczające państwo członkowskie może zgodnie z prawem krajowym narzucić warunki dotyczące sposobu wykorzystania takich danych i informacji przez otrzymujące państwo członkowskie, które musi takie warunki spełnić.

1.5.4. Krajowe punkty kontaktowe utworzone na podstawie decyzji z Prüm – duże imprezy

Państwa członkowskie goszczące duże imprezy o wymiarze międzynarodowym muszą je zabezpieczyć zarówno pod względem porządku publicznego, jak i walki z terroryzmem. Zależnie od charakteru imprezy (wydarzenie polityczne, sportowe, społeczne, kulturalne lub inne) jeden z tych aspektów może mieć większe znaczenie niż drugi. Należy jednak rozważyć oba, choć raczej powinny to robić różne organy. Szczególną uwagę poświęca się zjawisku podróżujących niebezpiecznych przestępców, zwłaszcza w przypadku międzynarodowych meczów piłki nożnej.

Do celów prewencji kryminalnej oraz ochrony porządku publicznego i bezpieczeństwa publicznego, w związku z dużymi imprezami i podobnymi zgromadzeniami masowymi (o charakterze politycznym, sportowym, społecznym, kulturalnym lub innym), klęskami żywiołowymi i poważnymi wypadkami mającymi skutki transgraniczne, wyznaczone krajowe punkty kontaktowe przekazują sobie wzajemnie, na wniosek lub z własnej inicjatywy:

- dane nieosobowe, lub
- dane osobowe, jeżeli prawomocne wyroki skazujące lub inne okoliczności dają podstawy do przypuszczania, że osoby, których dane dotyczą, dopuszczają się czynów karalnych podczas przedmiotowego wydarzenia lub że zagrażają porządkowi i bezpieczeństwu publicznemu.

Dane osobowe można przetwarzać jedynie do powyższych celów i w odniesieniu do określonych wydarzeń, w związku z którymi zostały dostarczone. Dostarczone dane należy bezzwłocznie usunąć, gdy cele te zostały osiągnięte, w każdym razie po upływie nie więcej niż jednego roku. Informacje są przekazywane zgodnie z prawem krajowym dostarczającego państwa członkowskiego.

1.5.4.1. Podręcznik współpracy podczas ważnych imprez międzynarodowych¹²

Podręcznik ten zawiera wytyczne i wskazówki dla organów ścigania, których zadaniem jest zapewnienie bezpieczeństwa publicznego podczas dużych imprez, takich jak igrzyska olimpijskie lub inne większe imprezy sportowe, imprezy społeczne lub posiedzenia polityczne na wysokim szczeblu.

Podręcznik, który jest stale zmieniany i dostosowywany w świetle rozwoju optymalnych rozwiązań, zawiera wskazówki dotyczące zarządzania informacjami i zarządzania wydarzeniami, jak również oceny strategicznej związanej z danym wydarzeniem. Załączone standardowe formularze dotyczą:

- wniosków o wyznaczenie oficerów łącznikowych;
- analizy ryzyka związanego z ewentualnymi demonstrantami i innymi zgromadzeniami;
- dane dotyczące wymiany informacji dotyczących osób lub grup stanowiących zagrożenie terrorystyczne;
- wykazu dokumentów źródłowych;
- tabeli zawierającej informacje o stałych punktach kontaktowych ds. porządku publicznego.

1.6. Narodowe punkty informacyjne dla piłki nożnej (NFIP)¹³

Równoległe z krajowymi punktami kontaktowymi utworzonymi na podstawie decyzji z Prüm i ze szczególnym uwzględnieniem międzynarodowych meczów piłki nożnej, narodowy punkt informacyjny dla piłki nożnej (NFIP) w każdym państwie członkowskim ma za zadanie wymianę właściwych informacji oraz rozwijanie transgranicznej współpracy policyjnej. Informacje taktyczne, strategiczne i operacyjne mogą być wykorzystywane przez sam NFIP lub przekazywane właściwym organom lub służbom policyjnym.

Kontakty między służbami policyjnymi różnych państw uczestniczących w wydarzeniu są koordynowane, a w razie potrzeby organizowane przez NFIP. Wykorzystująca dane CIV (Centre for Information on Football Vandalism – centrum informacji o wandalizmie kibiców) strona internetowa dotycząca NFIP (www.nfip.eu) zawiera informacje i porady na temat istniejących prawnych i pozaprawnych możliwościach zapewniania bezpieczeństwa i ochrony w związku z meczami piłki nożnej.

¹² Zalecenie Rady 2007/C 314/02 z dnia 6 grudnia 2007 r. w sprawie Podręcznika współpracy podczas ważnych imprez międzynarodowych przeznaczonego dla policji i organów bezpieczeństwa, Dz.U. C 314 z 22.12.2007, s. 4.

¹³ Decyzja Rady 2002/348/WSiSW z dnia 25 kwietnia 2002 r. dotycząca bezpieczeństwa w związku z meczami piłki nożnej o charakterze międzynarodowym, Dz.U. L 121 z 8.5.2002, s. 1.

NFIP koordynuje przetwarzanie informacji dotyczących kibiców stanowiących ryzyko, by umożliwić przygotowanie i przyjęcie właściwych środków w celu utrzymania porządku publicznego w trakcie imprez piłkarskich. Takie informacje obejmują w szczególności szczegółowe dane osób stanowiących lub mogących stanowić zagrożenie dla porządku publicznego i bezpieczeństwa. Informacje należy wymieniać za pomocą formularzy¹⁴ zawartych w dodatku do podręcznika dotyczącego meczów piłki nożnej.

1.6.1. Podręcznik dotyczący meczów piłki nożnej¹⁵

Podręcznik dotyczący meczów piłki nożnej stanowi załącznik do rezolucji Rady 2006/C 322/01 i zawiera przykłady tego, w jaki sposób organy policji powinny współpracować na szczeblu międzynarodowym, by przeciwdziałać przemocy oraz zakłóceniom porządku podczas meczów piłki nożnej oraz by kontrolować te zjawiska. Podręcznik zawiera przede wszystkim zalecenia dotyczące:

- zarządzania informacjami przez siły policyjne;
- organizacji współpracy między siłami policyjnymi;
- listy kontrolnej dotyczącej polityki medialnej i strategii w zakresie komunikacji (policja/władze).

¹⁴ Decyzja Rady 2007/412/WSiSW z dnia 12 czerwca 2007 r. zmieniająca decyzję 2002/348/WSiSW dotyczącą bezpieczeństwa w związku z meczami piłki nożnej o charakterze międzynarodowym, Dz.U. L 155 z 15.6.2007, s. 76.

¹⁵ Rezolucja Rady w sprawie zaktualizowanego podręcznika zaleceń w zakresie międzynarodowej współpracy policyjnej oraz w zakresie działań prewencyjnych i kontrolnych związanych z aktami przemocy i zakłóceniami porządku podczas międzynarodowych meczów piłki nożnej, które dotyczą co najmniej jednego państwa członkowskiego („podręcznik UE w sprawie meczów piłki nożnej”) (2016/C 444/01), Dz.U. C 322 z 29.11.2006, s. 1–36.

1.7. Centra współpracy policyjno-celnej (PCCC)

PCCC są ustanawiane na mocy umów dwustronnych lub wielostronnych zgodnie z art. 39 ust. 4 konwencji wykonawczej do układu z Schengen (CISA). W umowach tych umawiające się strony określają podstawę swojej współpracy transgranicznej, w tym zadania, ramy prawne i procedury ustanawiania i funkcjonowania centrów. PCCC skupiają personel z krajów sąsiadujących i są ściśle powiązane z organami krajowymi zajmującymi się współpracą międzynarodową (krajowymi punktami kontaktowymi, krajowymi biurami Interpolu, jednostkami krajowymi Europolu i biurami SIRENE).

Centra te udzielają porad i nieoperacyjnego wsparcia krajowym policyjnym jednostkom operacyjnym, organom celnym i innym agencjom w obszarze przygranicznym, w którym są położone. Zadaniem personelu PCCC jest szybkie dostarczanie informacji, o które zwrócono się zgodnie z decyzją Rady 2006/960/WSiSW („szwedzką decyzją ramową”).

Na początku 2016 roku do SIENA, czyli aplikacji sieci bezpiecznej wymiany informacji w Europolu, podłączono 8 z 59 istniejących PCCC. Informacje wymieniane za pośrednictwem PCCC dotyczą w szczególności przestępstw o drobnej i średniej wadze, przepływów migracji nieuregulowanej i zakłóceń porządku publicznego. Informacje takie mogą zawierać dane identyfikacyjne kierowców lub weryfikację stosowności i autentyczności dokumentów identyfikacyjnych i dokumentów podróży.

Umawiające się strony mogą – zwłaszcza w przypadku zdarzeń regionalnych (klęski żywiołowe) lub dużych imprez (igrzyska olimpijskie, puchar świata w piłce nożnej itp.) – wspólnie podjąć decyzję o przekształceniu PCCC w regionalne centrum koordynacji operacyjnej służące wszystkim zainteresowanym agencjom.

Jeżeli PCCC otrzyma informacje podlegające kompetencjom centralnych jednostek krajowych, musi je niezwłocznie przekazać do SPOC lub jednostki centralnej. Jeżeli PCCC otrzyma informacje z oczywistych względów interesujące Europol, może przekazać je jednostce krajowej Europolu działającej w ramach SPOC, która przekaze je do samego Europolu.

Przykład wymiany informacji za pośrednictwem PCCC

EPICC („Euroregionalne centrum informacji i współpracy policyjnej”) jest skrótowną nazwą PCCC Heerlen.

Utworzono je ad hoc (czyli nie na mocy konkretnego instrumentu prawnego) w 2005 r., z inicjatywy „NeBeDeAgPol”, stowarzyszenia szefów policji euroregionu delty Renu i Mozy, położonego w przygranicznym obszarze Niderlandów, Belgii i Niemiec – jednym z najgęściej zaludnionych obszarów przygranicznych w Unii Europejskiej.

W ramach tego PCCC na jednej platformie współpracuje około trzydziestu funkcjonariuszy policji belgijskiej, niemieckiej i holenderskiej.

Funkcjonariusze ci mają na miejscu dostęp do większości danych zawartych w ich krajowych bazach danych. Umożliwia im to przekazywanie – w bardzo krótkim czasie – rzetelnych, kompletnych i wiarygodnych odpowiedzi na policyjne wnioski o udzielenie informacji pochodzące z Belgii, Niemiec i Niderlandów. Wymiana informacji między trzema częściami EPICC odbywa się za pośrednictwem wykorzystywanego przez Europol systemu SIENA.

EPICC gromadzi i analizuje dostępne informacje policyjne w regionie przygranicznym, aby wykrywać, opisywać i rozwiązywać problemy związane z bezpieczeństwem granic (nowe zjawiska lub modus operandi, grupy przestępcze działające w regionie przygranicznym, wydarzenia lub osoby wymagające szczególnej uwagi itd.).

Dzięki swojej wiedzy fachowej i mieszanemu składowi PCCC Heerlen może zapewniać skuteczne wsparcie podczas przygotowywania i prowadzenia transgranicznych operacji, dochodzeń lub nadzoru.

1.8. Oficerowie łącznikowi

Zgodnie z art. 47 konwencji wykonawczej do układu z Schengen (CISA) państwa członkowskie „mogą zawierać umowy dwustronne przewidujące oddelegowanie, na czas określony lub nieokreślony, oficerów łącznikowych z jednego państwa [członkowskiego] do organów policji innego państwa [członkowskiego]”. Rolą oficerów łącznikowych jest nawiązywanie i utrzymywanie bezpośrednich kontaktów z myślą o nasileniu i przyspieszeniu współpracy w celu zwalczania przestępczości, szczególnie poprzez udzielanie pomocy. Oficerowie łącznikowi nie są uprawnieni do niezależnego wykonywania jakichkolwiek czynności policyjnych. Dzięki osobistym kontaktom i wzajemnemu zaufaniu zapewniają szybką i efektywną współpracę poprzez:

- ułatwianie i przyspieszanie zbierania i wymiany informacji;
- odpowiadanie na wnioski o pomoc policyjną oraz sądową w sprawach karnych;
- organizowanie i zapewnianie przeprowadzania operacji transgranicznych.

Oficerowie łącznikowi mogą być delegowani do innych państw członkowskich, państw trzecich, agencji UE lub organizacji międzynarodowych. Kompendium wiedzy¹⁶ na temat oficerów łącznikowych organów ścigania, corocznie aktualizowane przez Sekretariat Generalny Rady, opisuje funkcje i zadania oficerów łącznikowych oraz zawiera wykaz oficerów łącznikowych, wraz z danymi kontaktowymi.

W oparciu o przeszłe i bieżące doświadczenia zebrane w poszczególnych państwach przyjmujących i w celu lepszego połączenia działań państw członkowskich wobec państw trzecich pod względem zarówno pracy oficerów łącznikowych, jak i współpracy technicznej, określono różne dobre praktyki, które przedstawiono w kompendium. Proponuje się, by oficerowie łącznikowi państw członkowskich i ich właściwe organy stosowały te praktyki w stosownych przypadkach.

¹⁶ „Uaktualnione kompendium wiedzy na temat oficerów łącznikowych organów ścigania (2014)”, 11996/14 ENFOPOL 221 JAIEX 55 COMIX 384.

Typowe przykłady wymiany informacji między oficerami łącznikowymi

- *Oficerom łącznikowym można zlecać zapewnianie kontaktu w celu ustanowienia bezpośredniej współpracy w konkretnych przypadkach, takich jak przestępstwa związane z narkotykami.*
- *Oficerowie łącznikowi mogą dostarczać szczegółowych informacji na temat zasad i przepisów krajowych dotyczących międzynarodowej współpracy policyjnej lub pomocy prawnej w sprawach karnych.*
- *W niektórych przypadkach oficerowie łącznikowi utrzymują aktualne wykazy właściwych organów w danym państwie członkowskim.*
- *Oficerom łącznikowym zlecono również w niektórych państwach członkowskich rozpatrywanie wniosków dotyczących współpracy na mocy art. 17 decyzji z Prüm (wspólne działania). Na przykład Republika Czeska wystąpiła do duńskiego oficera łącznikowego w Europolu o przekazanie do Danii wniosku o wyznaczenie czterech duńskich funkcjonariuszy policji do uczestnictwa w sprawie dotyczącej obu tych państw członkowskich.*

1.9. Biura państw członkowskich ds. odzyskiwania mienia

Przestępczość finansowa obejmuje szeroki zakres działań: podrabianie, korupcję i oszustwa (np. oszustwa związane z kartami kredytowymi, oszustwa związane z kredytem hipotecznym, opieką medyczną i papierami wartościowymi; przekupstwo lub sprzeniewierzenie środków finansowych, pranie pieniędzy, kradzież tożsamości i oszustwa podatkowe). Lepszą współpracę osiąga się poprzez ściślejszą współpracę transgraniczną między biurami ds. odzyskiwania mienia (ARO), jednostkami analityki finansowej (FIU), policją i organami celnymi¹⁷.

Po przyjęciu decyzji Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotyczącej współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem¹⁸ wszystkie państwa członkowskie ustanowiły i wyznaczyły biura ds. odzyskiwania mienia (ARO). Te wyspecjalizowane jednostki przekształciły się w zwartą sieć specjalistów, którzy mogą bezpośrednio wymieniać za pośrednictwem systemu SIENA informacje w sprawach dotyczących odzyskiwania mienia. Pod auspicjami Komisji Europejskiej i Europolu sieć ARO ułatwia współpracę pomiędzy biurami ds. odzyskiwania mienia państw członkowskich oraz strategiczną dyskusję oraz wymianę optymalnych rozwiązań. Będący częścią Europolu urząd ds. mienia pochodzącego z działalności przestępczej (Criminal Assets Bureau – ECAB) działa jako centralny punkt kontaktowy do spraw odzyskiwania mienia w obrębie UE.

Przepisy określone w dyrektywie Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej¹⁹ przyczynią się do zwiększenia skuteczności współpracy między biurami ds. odzyskiwania mienia w Unii Europejskiej. Państwa członkowskie wezwano do dokonania transpozycji dyrektywy do 4 października 2016 r.

¹⁷ Podręcznik dobrych praktyk w zwalczaniu przestępstw finansowych: zbiór wzorcowych przykładów istniejących w państwach członkowskich dobrze rozwiniętych systemów służących zwalczaniu przestępstw finansowych, 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144.

¹⁸ Decyzja Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotycząca współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem, Dz.U. L 332 z 18.12.2007, s. 103.

¹⁹ Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej, Dz.U. L 127 z 29.4.2014, s. 39.

Międzyagencyjna Sieć Odzyskiwania Mienia Camden (CARIN), ustanowiona w 2004 r., by wspierać transgraniczną identyfikację, zamrażanie, zajmowanie i konfiskatę mienia związanego z przestępstwem, zwiększa wymianę informacji dotyczących różnych krajowych strategii, która wykracza poza UE.

Od 2015 r. sieć CARIN obejmuje specjalistów z 53 jurysdykcji i dziewięciu organizacji międzynarodowych, którzy działają jako punkty kontaktowe do celów szybkiej transgranicznej wymiany informacji na wniosek lub z własnej inicjatywy. Krajowe biura ds. odzyskiwania mienia współpracują ze sobą lub z innymi organami, ułatwiając ustalanie pochodzenia i identyfikację korzyści pochodzących z przestępstwa. Chociaż wszystkie państwa członkowskie utworzyły biura ds. odzyskiwania mienia, istnieją duże różnice między państwami członkowskimi, jeżeli chodzi o strukturę organizacyjną, zasoby i działania tych jednostek.

Informacje uzyskane w ramach wymiany mogą być wykorzystywane zgodnie z przepisami o ochronie danych otrzymującego je państwa członkowskiego oraz podlegają takim samym przepisom o ochronie danych, jak gdyby zostały pozyskane w otrzymującym je państwie członkowskim. Należy propagować spontaniczną wymianę informacji zgodnie z tą decyzją, z zastosowaniem procedur i terminów przewidzianych w szwedzkiej decyzji ramowej.

1.10. Pranie pieniędzy – współpraca między jednostkami analityki finansowej (FIU)²⁰²¹

Do krajowych jednostek analityki finansowej (FIU) należy zgłaszać istotne informacje dotyczące wszelkich faktów mogących świadczyć o praniu pieniędzy lub finansowaniu terroryzmu. Jednostki analityki finansowej analizują – w każdym przypadku indywidualnie – otrzymane informacje, aby ustalić powiązania między podejrzanymi transakcjami i leżącymi u ich podstaw działaniami przestępczymi, w celu zapobiegania praniu pieniędzy i finansowaniu terroryzmu oraz ich zwalczania. Jednostka analityki finansowej jest centralną jednostką krajową otrzymującą informacje, analizującą je i przesyłającą do właściwych organów wyniki swoich analiz. Jako że z punktu widzenia operacyjnego jest ona niezależna i autonomiczna, wypełnia ona swoje funkcje w sposób swobodny, co dotyczy również podejmowania autonomicznych decyzji dotyczących analizowania, żądania i rozpowszechniania określonych informacji.

²⁰ Decyzja Rady 2000/642/WSiSW z dnia 17 października 2000 r. dotycząca uzgodnień w sprawie współpracy pomiędzy jednostkami wywiadu finansowego państw członkowskich w odniesieniu do wymiany informacji, Dz.U. L 271 z 24.10.2000, s. 4.

²¹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 658/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE, Dz.U. L 141 z 5.6.2015, s. 73.

Jednostki analityki finansowej pełnią również rolę krajowych punktów kontaktowych przy transgranicznej wymianie informacji. Tak jak biura ds. odzyskiwania mienia także FIU w poszczególnych państwach członkowskich różnią się znacząco między sobą pod względem struktury organizacyjnej, funkcji i zasobów. Jednostki analityki finansowej znajdują się w strukturze organów sądowych lub organów policji, lub są tworzone jako organy hybrydowe, łączące kompetencje policji i prokuratury. Ta różnorodność może czasami utrudniać współpracę międzynarodową.

Z uwagi na międzynarodowy charakter prania pieniędzy i finansowania terroryzmu niezmiennie ważne są koordynacja i współpraca między jednostkami analityki finansowej. W celu usprawnienia takiej koordynacji i współpracy oraz dla zadbania o to, by raporty na temat podejrzanych transakcji docierały do jednostki analityki finansowej w państwie członkowskim, w której będą najbardziej przydatne, w dyrektywie (UE) 2015/849 sformułowano szczegółowe przepisy. Aby współpraca transgraniczna mogła odbywać się szybko, konstruktywnie i skutecznie w jak najszerszym zakresie, państwa członkowskie powinny w szczególności zadbać o to, by ich jednostki analityki krajowej wymieniały się informacjami z jednostkami analityki finansowej z państw trzecich w sposób swobodny, samorzutnie lub na żądanie.

Usprawnienie wymiany informacji pomiędzy jednostkami analityki finansowej w ramach Unii, korzystanie z bezpiecznych obiektów, w szczególności ze zdecentralizowanej sieci komputerowej FIU.NET. Do FIU.NET podłączono wszystkie 28 jednostek analityki finansowej. Sieć rozwinęła się w ostatnich latach, przekształcając się z bezpiecznego podstawowego narzędzia do uporządkowanej dwustronnej wymiany informacji w bezpieczne wielofunkcyjne narzędzie wielostronnej wymiany informacji, obejmujące elementy zarządzania sprawami oraz półautomatyczną standaryzację procesów. W FIU.NET każdy nowy element i zautomatyzowany proces są fakultatywne, a jednostki nie są zobowiązane do ich stosowania. Poszczególne jednostki analityki finansowej mogą podjąć decyzję, z jakich możliwości i elementów udostępnianych w ramach FIU.NET korzystają. Wykorzystują jedynie te elementy, które im odpowiadają, wyłączając te, których nie potrzebują lub których nie chcą.

1.11. Konwencja neapolitańska II²²

Państwa członkowskie udzielają sobie pomocy w ramach konwencji neapolitańskiej II w celu zapobiegania naruszeniom krajowych przepisów celnych i wykrywania takich naruszeń oraz w celu ścigania i karania naruszeń wspólnotowych i krajowych przepisów celnych. Jeżeli chodzi o dochodzenia w sprawach karnych, konwencja ustanawia procedury, dzięki którym administracje celne mogą współdziałać oraz wymieniać, z własnej inicjatywy lub na wniosek, dane dotyczące nielegalnego handlu.

Wnioski składa się w formie pisemnej w języku urzędowym państwa członkowskiego, w którym znajduje się organ będący adresatem wniosku, lub w języku akceptowanym przez ten organ. Istnieje formularz określający standard przekazywania informacji. Właściwe organy przekazują wszystkie informacje, które mogą pomóc w zapobieganiu naruszeniom oraz ich wykrywaniu i ściganiu. Wymieniają między sobą dane osobowe, czyli wszelkie informacje dotyczące osoby fizycznej, która jest zidentyfikowana lub możliwa do zidentyfikowania.

Organ będący adresatem wniosku lub powiadomiony przez niego właściwy organ, udzielając pomocy, postępuje tak, jakby działał na swoją rzecz lub na wniosek innego organu swojego państwa członkowskiego.

Podręcznik dotyczący konwencji neapolitańskiej II w sprawie pomocy wzajemnej i współpracy między administracjami celnymi jest podzielony na trzy części, które przedstawiają:

- postanowienia ogólne – dok. 13615/05 ENFOCUSTOM 61 + COR 1 (CZ);
- zestawienia informacyjne dotyczące poszczególnych państw, w wersji zaktualizowanej w 2016 r. – dok. 15429/16 JAI 1028 ENFOCUSTOM 238;
- załączniki, w tym standardowe formularze do przekazywania informacji – dok. 13615/05 ENFOCUSTOM 61 ADD 1.

²² Akt Rady z dnia 18 grudnia 1997 r. ustanawiający na podstawie artykułu K.3 Traktatu o Unii Europejskiej Konwencję w sprawie pomocy wzajemnej i współpracy między administracjami celnymi, Dz.U. C 24 z 23.1.1998, s. 1.

1.12. Jednostka do spraw informacji o pasażerach (PIU)

W ramach dyrektywy 2016/681²³ każde państwo członkowskie ustanawia lub wyznacza jednostkę do spraw informacji o pasażerach (JIP)²⁴. Jednostki te są uprawnione do przetwarzania danych o przelocie pasażera (danych PNR) otrzymanych od przewoźników lotniczych²⁵; stanowią także główny kanał wymiany informacji między państwami członkowskimi a Europolem. Dwa państwa członkowskie lub większa ich liczba mogą ustanowić lub wyznaczyć jeden organ jako swoją wspólną jednostkę JIP.

Przetwarzanie danych PNR służy przede wszystkim ocenie pasażerów linii lotniczych w celu identyfikacji osób, które powinny być poddane dalszemu sprawdzeniu przez krajowe organy właściwe do celów zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

Przedmiotowa dyrektywa ma zastosowanie do lotów pozaunijnych, ale może być też stosowana do lotów wewnątrzunijnych, jeśli państwo członkowskie tak postanowi.

Sprawdzenie danych PNR umożliwia identyfikację osób, które przed dokonaniem takiego sprawdzenia nie były podejrzewane o udział w przestępstwach terrorystycznych lub w poważnej przestępczości. Zgodnie z polityką UE w zakresie ochrony danych przetwarzanie przedmiotowych danych powinno być istotne i konieczne oraz proporcjonalne do szczególnych celów dotyczących bezpieczeństwa, którym służy ta dyrektywa.

²³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, Dz.U. L 119 z 4.5.2016, s. 132.

²⁴ Do dnia 25 maja 2018 r. państwa członkowskie wprowadzają w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania tej dyrektywy.

²⁵ Nie wpływa ona na możliwość ustanowienia przez państwa członkowskie, na mocy przepisów krajowych, systemu zbierania i przetwarzania danych PNR przekazywanych przez podmioty gospodarcze niebędące przewoźnikami, takie jak biura podróży i organizatorzy wycieczek świadczący usługi związane z podróżowaniem, w tym rezerwację lotów, na potrzeby których zbierają i przetwarzają dane PNR, lub przez dostawców usług transportowych innych niż dostawcy określani w tej dyrektywie, pod warunkiem że takie przepisy krajowe są zgodne z prawem Unii.

JIP są odpowiedzialne za:

- na szczeblu krajowym – gromadzenie danych PNR otrzymanych od przewoźników lotniczych, ich przechowywanie i przetwarzanie oraz przekazywanie tych danych lub wyników ich przetwarzania właściwym organom krajowym;
- na szczeblu UE – wymianę danych PNR i wyników ich przetwarzania:
 - a) pomiędzy sobą. W nagłych przypadkach i pod pewnymi warunkami wspomniane powyżej właściwe organy krajowe mogą jednak poprosić JIP innego państwa członkowskiego o bezpośrednie przekazanie im danych PNR przechowywanych w bazie danych tej jednostki; oraz
 - b) z Europol, który jest uprawniony – w granicach swojej kompetencji i na potrzeby realizowanych zadań – do zwracania się z wnioskiem do JIP o przekazanie danych PNR.

Jednostki do spraw informacji o pasażerach wykonują swoje zadania wyłącznie w bezpiecznej lokalizacji na terytorium danego państwa członkowskiego. Dane PNR przesłane do JIP muszą być przechowywane w bazie danych przez okres pięciu lat od momentu ich przekazania do JIP państwa członkowskiego przylotu lub wylotu. Jednak 6 miesięcy po ich przekazaniu wszystkie dane PNR muszą zostać poddane depersonalizacji poprzez maskowanie elementów danych określonych w dyrektywie i mogących posłużyć do bezpośredniego zidentyfikowania osoby, której dane dotyczą. Wyniki przetwarzania są przechowywane przez JIP wyłącznie przez okres niezbędny do poinformowania o pozytywnym wyniku właściwych organów oraz JIP w pozostałych państwach członkowskich.

JIP przetwarza wyłącznie dane PNR wymienione w załączniku I do dyrektywy w następujących celach:

- dokonania sprawdzenia pasażerów przed ich planowanym przylotem do państwa członkowskiego lub odlotem z niego w celu identyfikacji osób, które wymagają dalszego sprawdzenia przez organy krajowe, oraz – w stosownych przypadkach – przez Europol;
- odpowiadania, na podstawie oceny każdego indywidualnego przypadku, na wnioski właściwych organów o przekazanie i przetwarzanie danych PNR w związku z konkretnymi przypadkami oraz o przekazanie właściwym organom i – w stosownych przypadkach – Europolowi wyników takiego przetwarzania;
- analizowania danych PNR do celów aktualizacji lub tworzenia nowych kryteriów stosowanych do identyfikacji pasażerów mogących mieć związek z terroryzmem lub przestępczością zorganizowaną.

Dokonując przedmiotowego sprawdzania, JIP może porównywać dane PNR z bazami danych, które mają znaczenie dla zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, zgodnie z przepisami unijnymi, międzynarodowymi i krajowymi mającymi zastosowanie do takich baz danych lub przetwarzać dane PNR według wcześniej ustalonych kryteriów. Kryteria te muszą być ukierunkowane, proporcjonalne i szczegółowe. JIP, we współpracy z odpowiednimi właściwymi organami, ustala takie kryteria i dokonuje ich regularnego przeglądu. Kryteriów tych nie ustala się w oparciu o szczególnie chronione dane osobowe, takie jak rasa czy pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne czy orientacja seksualna danej osoby.

W odniesieniu do zidentyfikowanych osób, JIP przekazuje wszystkie istotne i niezbędne dane PNR lub wyniki ich przetwarzania swoim odpowiednikom w innych państwach członkowskich. Jednostki te przekazują otrzymane informacje swoim właściwym organom.

Inspektor ochrony danych powołany przez JIP odpowiada za monitorowanie przetwarzania danych PNR. Osoba, której dane dotyczą, ma prawo do kontaktowania się z inspektorem ochrony danych, jako pojedynczym punktem kontaktowym, we wszystkich sprawach związanych z przetwarzaniem jej danych PNR.

Każde przekazanie danych PNR przez przewoźników lotniczych do JIP odbywa się za pomocą środków elektronicznych, które zapewniają bezpieczeństwo pod względem technicznym. W tym celu na poziomie UE zostały określone²⁶ zarówno wspólne protokoły, których będą musieli przestrzegać przewoźnicy lotniczy podczas przekazywania danych, jak i obsługiwane formaty danych zapewniające możliwość ich odczytania przez wszystkie uczestniczące strony.

²⁶ Decyzja wykonawcza Komisji (UE) 2017/759 z dnia 28 kwietnia 2017 r. w sprawie wspólnych protokołów i formatów danych, z których mają korzystać przewoźnicy lotniczy podczas przekazywania danych dotyczących przelotu pasażera jednostkom do spraw informacji o pasażerach, Dz.U. L 113 z 29.4.2017, s. 48.

1.13. Wybór kanału – powszechnie stosowane kryteria

W państwie członkowskim SPOC²⁷ odgrywa podstawową rolę w określaniu najodpowiedniejszego i stosownego kanału, gdyż gromadzi wszystkie wnioski (zarówno przychodzące, jak i wychodzące) rozpatrywane przez daną jednostkę. W imię skuteczności organy krajowe pozostawiają prowadzącym dochodzenie znaczną autonomię w wyborze kanału, który wydaje się najwłaściwszy do celów dochodzenia. Najpowszechniej wykorzystywane kanały komunikacyjne to:

- SIRENE za pośrednictwem punktów kontaktowych każdego państwa Schengen dla SIS
- EUROPOL za pośrednictwem jednostek krajowych Europolu / oficerów łącznikowych Europolu
- INTERPOL za pośrednictwem krajowych biur Interpolu w komendach głównych policji
- oficerowie łącznikowi
- kanały wzajemnej pomocy wykorzystywane przez organy celne (konwencja neapolitańska II)
- kanały dwustronne oparte na umowach o współpracy na szczeblu krajowym, regionalnym i lokalnym (PCCC).

²⁷ Wytyczne dla pojedynczych punktów kontaktowych (SPOC), 10492/14 DAPIX 75 ENFOPOL 157 i 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1.

Ogólne zasady stanowią, że wniosek jest przekazywany tylko jednym kanałem. Jednak w wyjątkowych przypadkach wnioski mogą być przesyłane jednocześnie różnymi kanałami. W takich przypadkach należy to wyraźnie wskazać wszystkim stronom w odpowiedni sposób. Również o zmianie kanału należy poinformować wszystkie strony, podając powód zmiany. Aby uniknąć powielania tematów lub sytuacji, w których wniosek jest niepotrzebnie wysyłany wielokrotnie różnymi kanałami, właściwy urzędnik (SIS, Europol, Interpol, dwustronni oficerowie łącznikowi) w państwie występującym z wnioskiem może określić najodpowiedniejszą drogę dla wniosku o udzielenie informacji, kierując się następującymi kryteriami:

- **kryteria geograficzne** – gdy znane jest obywatelstwo / miejsce pobytu / pochodzenie danej osoby lub danego przedmiotu, a wniosek dotyczy przekazania szczegółowych informacji (adresu, numeru telefonu, odcisków palców, DNA, numeru rejestracyjnego itd.)
- **kryteria tematyczne** – przestępczość zorganizowana, poważna przestępczość, terroryzm; poufność / newralgiczność informacji; kanał wykorzystany w przypadku poprzednich powiązanych wniosków
- **kryteria techniczne** – gdy trzeba zapewnić bezpieczne kanały IT
- **kryteria pilności sprawy** – gdy dochodzi do bezpośredniego zagrożenia integralności fizycznej osoby, lub istnieje ryzyko utraty dowodów w najbliższym czasie, gdy wniosek dotyczy pilnych operacji transgranicznych lub nadzoru transgranicznego.

2. SYSTEMY INFORMACYJNE

2.1. System informacyjny Schengen drugiej generacji (SIS II)²⁸

System informacyjny Schengen drugiej generacji („SIS II”) działa obecnie w 26 państwach członkowskich UE oraz w czterech państwach niebędących członkami UE, które zostały włączone we współpracę Schengen: Norwegii, Islandii, Szwajcarii i Liechtensteinie. System wspiera współpracę operacyjną organów policji i organów sądowniczych w sprawach karnych. Ponieważ SIS jest systemem wspierającym zarówno współpracę policji, jak i organów kontroli granicznej, mogą z niego korzystać wyznaczeni funkcjonariusze policji, straży granicznej, służb celnych oraz organy wizowe i sądownicze w całej strefie Schengen.²⁹

Dane SIS II można wyszukiwać (pod warunkiem spełnienia restrykcyjnych warunków w zakresie ochrony danych) całodobowo za pośrednictwem punktów dostępu w biurach SIRENE, w punktach kontroli granicznej, na terytorium kraju i w konsulatach za granicą. W bazie znajdują się dane dotyczące **osób i przedmiotów**, co umożliwia wymianę danych do celów zapobiegania przestępczości i zwalczania imigracji nieuregulowanej. Dzięki wyszukiwaniu online w SIS urzędnik poszukujący informacji szybko ustala, czy jest „trafienie”, czyli czy w bazie danych znajduje się wpis na temat sprawdzanej osoby czy nie.

Dane mają formę wpisów, przy czym przez wpis rozumie się zestaw danych, które umożliwiają organom zidentyfikowanie osób lub przedmiotów z myślą o podjęciu stosownych działań.

Wpisy dotyczące **osób**, zarówno obywateli UE, jak i obywateli państw spoza UE. Umożliwiają one zastosowanie takich środków jak:

- aresztowanie danej osoby w celu jej wydania na podstawie europejskiego nakazu aresztowania lub umów zawieranych między UE a państwami trzecimi, lub w celu ekstradycji;
- wyszukiwanie miejsc pobytu osób zaginionych;
- wezwanie do stawienia się przed sądem w ramach postępowania karnego lub wykonania kary pozbawienia wolności;

²⁸ 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.

²⁹ Wykaz właściwych organów krajowych, które mają prawo dostępu do wpisów, jest corocznie publikowany w *Dzienniku Urzędowym Unii Europejskiej*.

- niejawna obserwacja i szczególne kontrole z myślą o zwalczaniu przestępstw karnych, zapobieganiu zagrożeniom bezpieczeństwa publicznego lub zapobieganiu zagrożeniom dla bezpieczeństwa narodowego;
- odmowa wjazdu na terytorium Schengen dla obywateli i cudzoziemców w wyniku decyzji administracyjnej lub sądowej lub ze względu na zagrożenie dla porządku publicznego lub bezpieczeństwa narodowego, lub ze względu na nieprzestrzeganie przepisów krajowych dotyczących wjazdu i pobytu cudzoziemców.

Wpisy w SIS II dotyczące **przedmiotów** są wprowadzane do celów kontroli niejawnych lub szczególnych, w celu zajęcia danego przedmiotu, wykorzystania go jako dowód w postępowaniu karnym lub w celu jego nadzorowania. Wpisy te mogą dotyczyć:

- pojazdów, łodzi, statków powietrznych, kontenerów,
- broni palnej,
- skradzionych dokumentów,
- banknotów,
- skradzionych przedmiotów, takich jak: dzieła sztuki, łodzie, statki.

Specjalnie upoważniony personel Europolu ma prawo, w granicach swojego mandatu, uzyskać dostęp i bezpośrednio wyszukiwać dane wprowadzone do SIS II i może zażądać dodatkowych informacji od danego państwa członkowskiego.

Krajowi przedstawiciele oddelegowani do Eurojustu oraz ich asystenci mają prawo, w granicach swojego mandatu, uzyskać dostęp do danych wprowadzonych do SIS II i je wyszukiwać.

2.2. EIS – system informacyjny Europolu³⁰

Rozporządzenie w sprawie Europolu wprowadza nową koncepcję przetwarzania danych, która jest często nazywana „koncepcją zintegrowanego zarządzania danymi”. Koncepcję zintegrowanego zarządzania danymi można zdefiniować jako możliwość wykorzystywania informacji związanych z przestępstwem na potrzeby wielu działań, wskazanych przez właściciela danych, co pozwala na zarządzanie tymi danymi i ich przetwarzanie w sposób zintegrowany, neutralny pod względem technologicznym. Na mocy decyzji Rady w sprawie Europolu przetwarzanie danych zostało tak pomyślane, by to poszczególne systemy stanowiły jego trzon. Rozporządzenie w sprawie Europolu nie zawiera już odniesień do systemów, ale w zamian wymaga wskazania celów przetwarzania. Aby użytkownicy mogli płynnie przechodzić na tę drugą metodę działania, mogą nadal korzystać z istniejących systemów, ale muszą z nimi pracować w sposób zgodny z nowymi ramami prawnymi.

System informacyjny Europolu (EIS), o którym mowa w decyzji w sprawie Europolu, to prowadzony przez Europol scentralizowany system, który umożliwia państwom członkowskim oraz partnerom współpracującym z Europolem przechowywanie, udostępnianie i kontrolę krzyżową danych dotyczących podejrzanych, skazanych lub potencjalnych przyszłych przestępców zamieszanych w przestępstwa podlegające kompetencji Europolu (poważna przestępczość, przestępczość zorganizowana lub terroryzm). System umożliwia przechowywanie pełnego zakresu danych i dowodów dotyczących tych przestępstw lub osób, np. nazwiska i pseudonimy, nazwy przedsiębiorstw, numery telefonów, adresy poczty elektronicznej, dane dotyczące pojazdów, broni, DNA, zdjęcia, odciski palców, informacje o bombach itp. EIS, który służy przede wszystkim jako system wspierający sprawdzanie krzyżowe, zapewnia dostęp w oparciu o trafienia (trafienie / brak trafienia). Rozporządzenie w sprawie Europolu przewiduje pełny dostęp do danych dostarczonych na potrzeby analizy do celów strategicznych lub tematycznych, ale już w przypadku danych, które zostały przekazane do celów analizy operacyjnej jest to wyłącznie dostęp w oparciu o trafienia (trafienie / brak trafienia).

³⁰

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. 53–114 (mające zastosowanie od 1 maja 2017 r.)

EIS jest de facto systemem referencyjnym pozwalającym stwierdzić, czy poszukiwane informacje są dostępne w jednym z państw członkowskich UE, u partnerów współpracujących z Europolu lub w samym Europolu. Jest on bezpośrednio dostępny we wszystkich państwach członkowskich. Dostęp do niego mają też odpowiednio upoważnieni pracownicy Europolu. Obecnie można wyróżnić trzy sposoby wprowadzania danych przez państwa członkowskie:

- a) wprowadzanie danych do EIS ręcznie lub poprzez aplikację SIENA;
- b) półautomatyczne przekazywanie danych poprzez ładowanie do EIS całej partii plików;
- c) automatyczne przekazywanie danych przy użyciu automatycznego systemu ładowania danych.

Zdecydowana większość danych w systemie informacyjnym Europolu (EIS) jest wprowadzana za pomocą automatycznych systemów ładowania danych. Zmieniło się podejście państw członkowskich do gromadzenia danych – jeśli chodzi o przekazywanie danych, nacisk kładzie się teraz na dane podmiotów, które mogą zostać zestawione, takich jak osoby, samochody, numery telefonów i broń palna.

Państwa trzecie nie mogą wprowadzać danych bezpośrednio do EIS, nie mogą także przeprowadzać w tym systemie sprawdzeń krzyżowych. Zgodnie z art. 23 ust. 5 rozporządzenia w sprawie Europolu mogą one jednak przekazywać dane Europolowi. Europol musi najpierw sprawdzić, czy dane są objęte zakresem jego mandatu. Jeśli tak, akceptuje te dane i przeprowadza sprawdzanie krzyżowe.

EIS, który umożliwia wymianę informacji wysoce wrażliwych, ma rozbudowany system zapewniający poufność i bezpieczeństwo. Bezpieczeństwo zapewniają na przykład określone kody postępowania. Wskazują one, co można zrobić z danymi informacjami i kto ma do nich dostęp. Kody postępowania są zaprojektowane w taki sposób, by chronić źródło informacji i zapewniać, by przetwarzanie informacji odbywało się zgodnie z życzeniem właściciela informacji oraz zgodnie z prawem krajowym danego państwa członkowskiego. EIS jest upoważniony do przetwarzania danych do poziomu EU RESTRICTED włącznie.

2.3. SIENA – stworzona na potrzeby Europolu aplikacja sieci bezpiecznej wymiany informacji

SIENA jest bezpiecznym systemem łączności Europolu na użytek państw członkowskich, Europolu i partnerów z nim współpracujących do wymiany operacyjnych i strategicznych informacji i danych wywiadowczych mających związek z przestępstwami, w tym danych operacyjnych na temat osób. SIENA jest systemem przesyłania komunikatów, umożliwiającym przesyłanie różnych rodzajów wiadomości do różnych celów, w tym wymiany danych na mocy szwedzkiej decyzji ramowej.

W projektowaniu i funkcjonowaniu SIENA istotny nacisk położono na bezpieczeństwo, ochronę danych i poufność. SIENA jest systemem akredytowanym do wymiany informacji o klauzuli EU CONFIDENTIAL. W przypadku wymiany danych poprzez system SIENA zastosowanie mają jasno określone zasady dotyczące przetwarzania danych. Dla każdej informacji wysyłanej poprzez system SIENA należy wskazać klasyfikację (poziom poufności), kody postępowania i wiarygodność źródła oraz informacji.

Językiem domyślnym interfejsu użytkownika systemu SIENA jest język angielski, a interfejs ten jest wielojęzyczny, co umożliwia operatorom systemu pracę w ich własnych językach narodowych. Oprócz wymiany komunikatów operatorzy systemu SIENA mogą wyszukiwać dane i tworzyć sprawozdania statystyczne na podstawie danych wymienianych za pośrednictwem tego systemu.

SIENA ułatwia dwustronną wymianę danych między państwami członkowskimi i umożliwia im wymianę danych poza mandatem Europolu. Gdy wymiana danych dotyczy jednego z partnerów współpracujących z Europolem, państwa członkowskie są powiadamiane za pośrednictwem systemu SIENA, że taka wymiana może mieć miejsce jedynie wtedy, gdy dotyczy przestępstw objętych mandatem Europolu.

Europol zajmuje się wymienianymi za pośrednictwem systemu SIENA informacjami niezbędnymi do celów przetwarzania danych operacyjnych, jedynie gdy jest włączony do takiej wymiany danych jako jeden z adresatów. Do celów audytu dostęp do wszystkich danych wymienianych poprzez system SIENA mają inspektor ochrony danych Europolu i krajowe organy nadzoru.

SIENA umożliwia usystematyzowaną wymianę danych w oparciu o uniwersalny format wiadomości (ang. Universal Message Format – UMF). Obecnie w internetowej aplikacji SIENA można stworzyć / wyświetlić encję UMF OSOBA. Usługa sieciowa SIENA obsługuje już pełny model danych w formacie UMF.

2.4. System I-24/7 – globalny policyjny system łączności Interpolu

System I-24/7, globalna sieć wymiany informacji policyjnych, łączy Sekretariat Generalny Interpolu w Lyonie, we Francji, z krajowymi biurami Interpolu w 190 krajach i biurach regionalnych.

System informacyjny Interpolu umożliwia bezpośrednie przekazywanie wiadomości pomiędzy krajowymi biurami Interpolu. Wszystkie bazy danych Interpolu (z wyjątkiem bazy obrazów dotyczących seksualnego wykorzystywania dzieci) są dostępne w czasie rzeczywistym za pośrednictwem systemu I-24/7, tj. globalnego policyjnego systemu łączności. System I-24/7 umożliwia również państwom będącym członkami organizacji wzajemny dostęp do ich krajowych baz danych przy użyciu łączy typu *business-to-business* (B2B). Państwa będące członkami organizacji zarządzają własnymi krajowymi danymi kryminalnymi, przechowują je i kontrolują ich przekazywanie, dostęp innych państw do tych danych i ich niszczenie zgodnie z swoimi przepisami krajowymi. Mogą również udostępniać je międzynarodowym organom ścigania za pośrednictwem systemu I-24/7.

2.4.1. Interpol: brama sieciowa DNA

Baza danych DNA Interpolu obejmuje międzynarodową bazę danych DNA, formularz wniosku poszukiwań międzynarodowych w wymianie dwustronnej i środki bezpiecznego ustandaryzowanego transferu elektronicznego. Nie przechowuje się żadnych danych nominalnych, które łączyłyby profile DNA z konkretną osobą. Brama sieciowa DNA jest kompatybilna z systemem zautomatyzowanej wymiany danych Prüm.

Państwa będące członkami organizacji mają dostęp do bazy danych, a na żądanie dostęp może być rozszerzany poza krajowe biura Interpolu w państwach będących członkami organizacji i obejmować ośrodki i laboratoria kryminalistyczne. Policja w państwach będących członkami organizacji może przedkładać profile DNA sprawców, profile z miejsc popełnienia przestępstwa, profile osób zaginionych i niezidentyfikowanych ciał.

2.4.2. Baza danych odcisków palców Interpolu

Upoważnieni użytkownicy w państwach będących członkami organizacji mogą przeglądać wpisy, zamieszczać je i sprawdzać krzyżowo za pośrednictwem automatycznego systemu identyfikacji daktyloskopijnej (AFIS). Wpisy są zachowywane i przesyłane w formacie określonym przez Narodowy Instytut Standaryzacji i Technologii (NIST). Wytyczne dotyczące przekazywania odcisków palców oraz wytyczne dotyczące przekazywania odcisków palców z miejsca przestępstwa pomagają państwom będącym członkami organizacji w poprawie jakości i zwiększaniu liczby wpisów dotyczących odcisków palców przekazywanych do AFIS Interpolu.

2.4.3. Baza zawierająca dane skradzionych lub utraconych dokumentów podróży

W bazie Interpolu zawierającej dane skradzionych lub utraconych dokumentów podróży przechowuje się informacje o ponad 45 milionach dokumentach podróży zgłoszonych przez 166 państw jako zagubione lub skradzione. Baza ta umożliwia krajowym biurom Interpolu i innym upoważnionym organom ścigania (takim jak służby imigracyjne i kontrola graniczna) weryfikowanie ważności podejrzanych dokumentów podróży. Właściwe organy ścigania w państwach członkowskich wymieniają z Interpolem dane o paszportach, by zapobiegać poważnej i zorganizowanej przestępczości oraz zwalczać te zjawiska³¹.

2.4.4. Tabela odniesienia Interpolu dotycząca broni palnej

Tabela odniesienia Interpolu dotycząca broni palnej umożliwia prowadzącym dochodzenie odpowiednie zidentyfikowanie broni palnej użytej do dokonania przestępstwa (marka, model, kaliber itp.). Baza zawiera ponad 250 000 wpisów dotyczących broni palnej i 57 000 wysokiej jakości obrazów. Sieć informacji balistycznych Interpolu jest platformą dużych międzynarodowych operacji wymiany i porównywania danych balistycznych, w której znajduje się ponad 150 000 wpisów.

System Interpolu do zarządzania rejestrowaniem i śledzeniem nielegalnej broni (iARMS) jest aplikacją informatyczną, która ułatwia wymianę informacji i współpracę między organami ścigania w zakresie przestępstw związanych z bronią palną.

³¹ Wspólne stanowisko Rady 2005/69/WSiSW w sprawie wymiany niektórych danych z Interpolem, Dz.U. L 27 z 29.1.2005, s. 61.

2.5. Europejski system przekazywania informacji z rejestrów karnych (ECRIS)³²

Komputerowy europejski system przekazywania informacji z rejestrów karnych (ECRIS)³³ zapewnia elektroniczne środki służące wymianie – w znormalizowanym formacie – informacji o wyrokach między państwami członkowskim. ECRIS jest wykorzystywany do powiadamiania państw członkowskich o wyrokach skazujących wydanych na ich obywateli i do przekazywania wniosków o informacje o wyrokach do celów postępowania karnego i do innych celów, np. administracyjnych lub związanych z zatrudnieniem. Istnieje również możliwość składania wniosków dotyczących obywateli państw trzecich, jeżeli istnieje powód, by przypuszczać, że państwo członkowskie, do którego wystąpiono z wnioskiem, posiada informacje na temat danej osoby.

Na wnioski składane za pośrednictwem systemu ECRIS należy odpowiedzieć w terminie 10 dni roboczych, jeżeli wniosek służy celom postępowań karnych lub zatrudnienia, i w terminie 20 dni roboczych, jeżeli wniosek złożyła osoba prywatna do własnych celów.

ECRIS nie został pomyślany jako scentralizowana baza danych rejestrów karnych i opiera się na zdecentralizowanej strukturze informatycznej, w której wszystkie rejestry karne są przechowywane wyłącznie w bazach danych obsługiwanych przez państwa członkowskie. Dane są wymieniane elektronicznie między wyznaczonymi organami centralnymi państw członkowskich.

Państwa członkowskie mają przysyłać informacje zgodnie z ustalonymi zasadami i w znormalizowanych formatach, w możliwie wyczerpującej formie, tak aby otrzymujące je państwo członkowskie mogło je właściwie przetworzyć i zidentyfikować daną osobę. Komunikaty są wysyłane w językach urzędowych danego państwa członkowskiego lub w innym języku akceptowanym przez oba państwa członkowskie.

Niewiążący podręcznik dla użytkowników, określający procedury wymiany informacji i koordynowania działań na rzecz rozwoju i funkcjonowania ECRIS jest publikowany przez Sekretariat Generalny Rady i jest dostępny w wersji elektronicznej na stronie internetowej Rady oraz na prowadzonej przez Komisję Europejską stronie CIRCABC pod adresem <https://circabc.europa.eu>. Wnioski o dostęp do podręcznika należy przysyłać do Sekretariatu Rady. Wnioski o dostęp do ograniczonej grupy „Działanie ECRIS oraz wsparcie techniczne” należy przysyłać do Komisji Europejskiej.

³² Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji, Dz.U. L 93 z 7.4.2009, s. 23.

³³ Decyzja Rady 2009/316/WSiSW w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), zgodnie z art. 11 decyzji ramowej 2009/315/WSiSW, Dz.U. L 93 z 7.4.2009, s. 33.

2.6. Wizowy system informacyjny (VIS)³⁴

Wizowy system informacyjny (VIS) jest przede wszystkim systemem kontroli imigracji. Jest on narzędziem ułatwiającym współpracę na poziomie kontroli granicznej za pośrednictwem elektronicznej weryfikacji i wymiany danych wizowych między państwami członkowskimi na granicach zewnętrznych UE. W związku z tym dotyczy przede wszystkim cudzoziemców. Wyznaczone organy państw członkowskich (tj. urzędy konsularne, przejścia graniczne, policja i organy imigracyjne)³⁵ i Europolu³⁶, w ramach swoich zadań, mogą korzystać z VIS³⁷ w celu zapobiegania następującym przestępstwom, ich wykrywania i ścigania:

- przestępstwa terrorystyczne, czyli te przestępstwa w rozumieniu prawa krajowego, które odpowiadają – lub są równoważne – przestępstwom określonym w art. 1–4 decyzji ramowej Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu, lub
- poważne przestępstwa, czyli te formy przestępczości, które odpowiadają – lub są równoważne – przestępstwom określonym w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW (europejski nakaz aresztowania).

Zgodnie ze szwedzką decyzją ramową informacje zgromadzone w VIS mogą być przekazywane Zjednoczonemu Królestwu i Irlandii przez właściwe organy tych państw członkowskich, których wyznaczone organy mają dostęp do VIS, a informacje zgromadzone w krajowych rejestrach wizowych Zjednoczonego Królestwa i Irlandii mogą być przekazywane właściwym organom ścigania innych państw członkowskich.

³⁴ Decyzja Rady z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS) (2004/512/WE), Dz.U. L 213 z 15.6.2004, s. 5.

³⁵ Wykaz właściwych organów, których odpowiednio upoważniony personel ma dostęp pozwalający wprowadzać, modyfikować, usuwać lub przeglądać dane w Wizowym Systemie Informacyjnym (VIS) (2016/C 187/04), Dz.U. C 187 z 26.5.2016, s. 4.

³⁶ Decyzja Rady (WE) nr 2008/633/WSiSW w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do wizowego systemu informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania, Dz.U. L 218 z 13.8.2008, s. 129; Decyzja Rady dotycząca wyznaczenia daty, od której staje się skuteczna decyzja 2008/633/WSiSW w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do wizowego systemu informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania (2013/392/UE), Dz.U. L 198 z 23.7.2013, s. 45.

³⁷ 16 kwietnia 2015 r. Trybunał Sprawiedliwości Unii Europejskiej unieważnił decyzję Rady 2013/392/UE z dnia 22 lipca 2013 r. dotyczącą wyznaczenia daty, od której staje się skuteczna decyzja 2008/633/WSiSW w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do wizowego systemu informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania. Jednocześnie Trybunał orzekł, że skutki decyzji 2013/392 zostają utrzymane do czasu wejścia w życie nowego aktu, który ją zastąpi.

VIS oparty jest na scentralizowanym systemie i wspólnej platformie z SIS II. Przetwarzanie danych w VIS przebiega w dwóch etapach. Na pierwszym etapie dane obejmują dane alfanumeryczne i zdjęcia. Na drugim – dane biometryczne i zeskanowane dokumenty są przetwarzane i wprowadzane do systemu VIS. W systemie VIS znajdują się dane dotyczące wniosków wizowych, zdjęć, odcisków palców, powiązanych decyzji organów wizowych oraz odsyłacze między powiązanymi aplikacjami. VIS wykorzystuje system porównywania danych biometrycznych, co zapewnia rzetelne porównanie odcisków palców do celów:

- weryfikacji, tj. sprawdzenia, czy odciski palców zeskanowane na przejściu granicznym odpowiadają odciskom palców znajdującym się w danych biometrycznych dołączonych do wizy, lub
- identyfikacji, tj. porównania odcisków palców pobranych na przejściu granicznym z odciskami znajdującymi się w całej bazie danych.

Z technicznego punktu widzenia VIS składa się z trzech następujących poziomów: centralnego, krajowego i lokalnego, który obejmuje urzędy konsularne, przejścia graniczne oraz organy policyjne i imigracyjne. VIS i SIS II wykorzystują tę samą platformę techniczną, tak aby dostęp do danych przez funkcjonariuszy obsługujących systemy był wzajemny, tj. by obsługujący VIS mieli dostęp do danych w SIS II i odwrotnie.

2.7. Eurodac^{38 39}

Europejski zautomatyzowany system identyfikacji odcisków palców (Eurodac) pomaga przede wszystkim określić państwo członkowskie odpowiedzialne za rozpatrywanie wniosków o udzielenie azylu złożonych w jednym z państw członkowskich oraz pod innymi względami ułatwia stosowanie konwencji dublińskiej. Dostęp do Eurodac na potrzeby prewencji w przypadku przestępstw terrorystycznych oraz innych poważnych przestępstw kryminalnych, ich wykrywania lub prowadzenia dochodzeń w ich sprawach jest udzielany jedynie w ściśle określonych przypadkach.

³⁸ Rozporządzenie Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczące ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej, Dz.U. L 316 z 15.12.2000, s. 1.

³⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona).

Rozporządzenie nr 603/2013 w sprawie Eurodac określa zasady przesyłania danych o odciskach palców do jednostki centralnej, zapisu takich danych oraz innych danych o istotnym znaczeniu w centralnej bazie danych, ich przechowywania, porównywania z innymi danymi o odciskach palców, przesyłania wyników takich porównań oraz blokowania i usuwania zarejestrowanych danych.

Struktura systemu Eurodac obejmuje: a) skomputeryzowaną centralną bazę danych odcisków palców („system centralny”) złożoną z jednostki centralnej oraz planu i systemu zachowania ciągłości działania oraz b) infrastrukturę komunikacyjną między systemem centralnym a państwami członkowskimi zapewniającą szyfrowaną wirtualną sieć służącą do przekazywania danych Eurodac („infrastruktura łączności”).

Każde państwo członkowskie posiada jeden krajowy punkt dostępu.

Agencja eu-LISA ustanowiona rozporządzeniem (UE) nr 1077/2011⁴⁰ odpowiada za zarządzanie operacyjne systemem Eurodac oraz zapewnia – we współpracy z państwami członkowskimi – stosowanie w systemie centralnym przez cały czas najlepszych i najbezpieczniejszych spośród dostępnych technologii i technik, z zastrzeżeniem analizy kosztów i korzyści.

Każde państwo członkowskie może przekazywać odciski palców do jednostki centralnej w celu sprawdzenia, czy cudzoziemiec w wieku co najmniej 14 lat, co do którego ustalono, że przebywa nielegalnie na jego terytorium, nie złożył już wniosku o udzielenie azylu w innym państwie członkowskim. Jednostka centralna porównuje te odciski palców z danymi daktyloskopijnymi przesłanymi przez inne państwa członkowskie i przechowywanymi już w centralnej bazie danych. Jednostka informuje państwo członkowskie, które przesłało dane, czy jest trafienie, czyli informuje o wyniku porównania odcisków palców zarejestrowanych i przekazanych. To państwo członkowskie sprawdza wynik i przystępuje do ostatecznej identyfikacji we współpracy z zainteresowanymi państwami członkowskimi.

Państwa członkowskie są zobowiązane do zapewnienia legalności, dokładności i bezpieczeństwa danych Eurodac. Każda osoba lub państwo członkowskie, które poniosły szkody w wyniku nieprzestrzegania przepisów Eurodac, jest uprawnione do otrzymania odszkodowania od państwa członkowskiego odpowiedzialnego za wyrządzoną szkodę.

⁴⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, Dz.U. L 286 z 1.11.2011, s. 1.

Rozporządzenie (UE) nr 603/2013 przewiduje dostęp do danych Eurodac przez wyznaczone organy państw członkowskich i Europol na potrzeby ochrony porządku publicznego. Zgodnie z rozporządzeniem wyznaczone organy mogą przedłożyć umotywowany elektroniczny wniosek o porównanie danych dotyczących odcisków palców z danymi przechowywanymi w systemie centralnym jedynie wówczas, gdy porównanie z poniższymi bazami danych nie doprowadziło do ustalenia tożsamości osoby, której dane dotyczą:

- krajowe bazy odcisków palców;
- automatyczne systemy identyfikacji daktyloskopijnej (AFIS) wszystkich innych państw członkowskich na mocy decyzji 2008/615/WSiSW („decyzje z Prüm”), w przypadku gdy porównanie jest technicznie możliwe, chyba że istnieją uzasadnione powody, by sądzić, iż porównanie z takimi systemami nie doprowadziłoby do ustalenia tożsamości osoby, której dane dotyczą. Takie uzasadnione powody podaje się w umotywowanym elektronicznym wniosku o porównanie z danymi Eurodac, przesłanym przez wyznaczony organ organowi weryfikującemu;
- wizowy system informacyjny (VIS), gdy spełnione są warunki takiego porównania ustanowione w decyzji 2008/633/WSiSW.

Muszą zostać spełnione także wszystkie następujące warunki:

- a) porównanie jest niezbędne na potrzeby zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub ścigania, co oznacza, że występują nadrzędne względy bezpieczeństwa publicznego, które sprawiają, że przeszukiwanie bazy danych jest współmierne do okoliczności;
- b) porównanie jest niezbędne w konkretnej sprawie (tzn. nie prowadzi się rutynowych porównań);
- c) istnieją uzasadnione powody, by sądzić, że porównanie znacznie przyczyni się do zapobieżenia wszelkim odnośnym przestępstwom, ich wykrycia lub ścigania. Takie uzasadnione powody istnieją w szczególności w przypadku, gdy zachodzi uzasadnione podejrzenie, że osoba podejrzana o popełnienie przestępstwa terrorystycznego lub innego poważnego przestępstwa, ich sprawca lub ofiara należą do jednej z kategorii objętych rozporządzeniem (UE) nr 603/2013.

2.8. CIS – system informacji celnej⁴¹

System informacji celnej stanowi uzupełnienie konwencji neapolitańskiej II⁴². System ten ma na celu usprawnienie administracji celnych państw członkowskich dzięki szybkiej wymianie informacji, z myślą o zapobieganiu poważnym naruszeniom przepisów prawa krajowego i wspólnotowego, prowadzeniu dochodzeń w ich sprawie i ich ścigania. CIS umożliwia również ustanowienie identyfikującej bazy danych rejestru celnego (FIDE), która ma ułatwiać prowadzenie dochodzeń celnych.

System CIS, którym zarządza Komisja, jest scentralizowanym systemem informacyjnym dostępnym poprzez terminale w każdym państwie członkowskim oraz w Komisji, Europolu i agencji Eurojust. Dostęp do danych CIS mogą uzyskać krajowe organy celne, podatkowe, rolne, zdrowia publicznego i organy policji, Europol i agencji Eurojust. Bezpośredni dostęp do danych zawartych w CIS mają wyłącznie organy wyznaczone przez państwa członkowskie⁴³ i Komisja. W celu zwiększenia komplementarności Europol i Eurojust mają dostęp do danych CIS i FIDE tylko w trybie do odczytu.

CIS zawiera dane osobowe w odniesieniu do towarów, środków transportu, przedsiębiorstw, osób i wyrobów, a także dóbr i środków pieniężnych, zatrzymanych, zajętych lub skonfiskowanych. Dane osobowe mogą być kopiowane z CIS do innych systemów przetwarzania danych w związku z zarządzaniem ryzykiem lub z analizami operacyjnymi, do których mają dostęp jedynie analitycy wyznaczeni przez państwa członkowskie.

FIDE umożliwia organom krajowym odpowiedzialnym za prowadzenie dochodzeń celnych, określenie – w momencie wszczęcia dochodzenia – innych organów, które mogły prowadzić dochodzenia w sprawie danej osoby lub przedsiębiorstwa.

⁴¹ Decyzja Rady 2009/917/WSiSW z dnia 30 listopada 2009 r. w sprawie stosowania technologii informatycznej do potrzeb celnych, Dz.U. L 323 z 10.12.2009, s. 20.

⁴² Konwencja sporządzona na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie pomocy wzajemnej i współpracy między administracjami celnymi, Dz.U. C 24 z 23.1.1998, s. 2.

⁴³ Wdrożenie art. 7 ust. 2 i art. 8 ust. 3 decyzji Rady 2009/917/WSiSW z dnia 30 listopada 2009 r. w sprawie stosowania technologii informatycznej do potrzeb celnych – zaktualizowany wykaz właściwych organów, 13394/11 ENFOCUSTOM 85.

2.9. Falszywe i autentyczne dokumenty online – FADO⁴⁴

Skomputeryzowany system archiwizacji obrazu, obejmujący dokumenty falszywe i autentyczne i oparty na technologii internetowej, umożliwia szybką i bezpieczną wymianę informacji między Sekretariatem Generalnym Rady Unii Europejskiej i osobami sprawdzającymi dokumenty we wszystkich państwach członkowskich, a także w Islandii, Norwegii i Szwajcarii. System umożliwia porównanie na ekranie dokumentu oryginalnego z dokumentem falszywym lub podrobionym. Zawiera przede wszystkim dokumenty państw członkowskich oraz dokumenty państw trzecich, w przypadku gdy z tych państw regularnie emigruje do państw członkowskich wiele osób. Baza danych stworzona przez FADO zawiera następujące dane:

- zdjęcia oryginalnych dokumentów;
- informacje na temat technik zabezpieczeń (zabezpieczenia);
- zdjęcia typowych falszywych i podrobionych dokumentów;
- informacje o technikach podrabiania dokumentów oraz
- dane statystyczne dotyczące wykrytych falszywych i sfalszowanych dokumentów oraz kradzieży tożsamości.

System wykorzystuje specjalne linie przesyłania danych między Sekretariatem Generalnym Rady i służbami centralnymi zlokalizowanymi w państwach członkowskich. W każdym państwie członkowskim odczytanie danych z systemu następuje za pośrednictwem służb centralnych za pomocą bezpiecznego połączenia internetowego. Państwo członkowskie może wykorzystywać taki system wewnątrz na swoim terytorium, co oznacza połączenie różnych stacji roboczych znajdujących się w poszczególnych punktach kontroli granicznej tego państwa lub w innych właściwych organach. Nie ma jednak bezpośredniego połączenia między stacjami roboczymi innymi niż krajowe służby centralne, a służby centralne w Sekretariacie Generalnym.

FADO działa obecnie w 22 językach urzędowych Unii Europejskiej. Dokumenty są wprowadzane przez ekspertów ds. dokumentów w dowolnym języku, a standardowe opisy są tłumaczone automatycznie. W związku z tym dokumenty są natychmiast dostępne we wszystkich obsługiwanych językach. Dodatkowe informacje tekstowe są następnie tłumaczone przez wyspecjalizowanych tłumaczy Sekretariatu Generalnego Rady.

⁴⁴ Wspólne działanie (98/700/WSiSW) z dnia 3 grudnia 1998 r. przyjęte przez Radę na podstawie artykułu K.3 Traktatu o Unii Europejskiej, dotyczące ustanowienia Europejskiego Systemu Archiwizacji Obrazu (FADO), Dz.U. L 333 z 9.12.1998, s. 4.

2.10. Publiczny rejestr on-line autentycznych dokumentów tożsamości i dokumentów podróży – PRADO

Podczas gdy dostęp do FADO jest ograniczony do osób sprawdzających dokumenty i do zastosowań rządowych, utrzymywany przez Radę Unii Europejskiej publiczny rejestr on-line autentycznych dokumentów tożsamości i dokumentów podróży (PRADO – **P**ublic **R**egister of **A**uthentic Travel and Identity **D**ocuments **O**nline) zawiera podzbiór informacji FADO udostępniany publicznie. Ta strona internetowa⁴⁵ jest – ze względu na przejrzystość – publikowana w językach urzędowych UE przez Sekretariat Generalny Rady Unii Europejskiej i zapewnia ważne usługi wielu użytkownikom w Europie, w szczególności organizacjom pozarządowym, które mają potrzebę lub prawny obowiązek sprawdzania czyjejś tożsamości.

Strona ta zawiera opisy techniczne, w tym informacje dotyczące zabezpieczeń stosowanych w autentycznych dokumentach tożsamości i dokumentach podróży. Informacje są wybierane i dostarczane przez ekspertów ds. dokumentów z państw członkowskich, Islandii, Norwegii i Szwajcarii.

Użytkownicy znajdą również w PRADO linki do stron internetowych z informacjami na temat numerów nieważnych dokumentów podanymi przez niektóre państwa członkowskie i państwa trzecie oraz inne przydatne informacje dotyczące sprawdzania tożsamości oraz kontroli dokumentów i oszustw w tym zakresie.

⁴⁵ <http://www.prado.consilium.europa.eu/>

2.11. Przegląd systemów informacyjnych stosowanych do unijnej wymiany informacji

Systemy informatyczne i bazy danych	Podstawa prawna	Cel	Osoby, których dane dotyczą	Udostępnianie danych
System informacyjny Schengen drugiej generacji – SIS II	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.	• Bezpieczeństwo wewnętrzne • Kontrola graniczna • Współpraca sądowa • Dochodzenie	• Obywatele UE • Obywatele państw trzecich	• VIS • Europol • Eurojust • Interpol
	Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz.U. L 381 z 23.12.2006, s. 4.	• Odmowa wjazdu lub pobytu • Polityka azylowa, imigracyjna i powrotowa	• Obywatele państw trzecich, którzy nie mają prawa do swobodnego przemieszczania się równego prawu, z którego korzystają obywatele UE	
Europol EIS	Decyzja Rady 2009/371/WSiSW z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji (Europol), art. 11–13, Dz.U. L 121 z 15.5.2009, s. 37.	• Poważna przestępczość • Imigracja • Bezpieczeństwo wewnętrzne • Zwalczanie terroryzmu	• Obywatele UE • Obywatele państw trzecich	• SIS II
Interpol System I-24/7	Konstytucja Interpolu		• Obywatele UE • Obywatele państw trzecich	• SIS II • Europol • VIS

Interpol Utracone lub skradzione dokumenty podróży (SLTD)	Wspólne stanowisko Rady 2005/69/WSiSW w sprawie wymiany niektórych danych z Interpolem, Dz.U. L 27 z 29.1.2005, s. 61.	• Przestępczość międzynarodowa i zorganizowana • Bezpieczeństwo wewnętrzne	• Obywatele UE • Obywatele państw trzecich	
ECRIS	Decyzja Rady 2009/316/WSiSW w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), zgodnie z art. 11 decyzji ramowej 2009/315/WSiSW, Dz.U. L 93 z 7.4.2009, s. 33.	Postępowanie karne	• Obywatele UE • Obywatele państw trzecich	

VIS	Decyzja Rady z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS) (2004/512/WE), Dz.U. L 213 z 15.6.2004, s. 5. Decyzja Rady (WE) nr 2008/633/WSiSW w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania, Dz.U. L 218 z 13.8.2008, s. 129. Decyzja Rady dotycząca wyznaczenia daty, od której staje się skuteczna decyzja 2008/633/WSiSW w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do wizowego systemu informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania, (2013/392/UE), Dz.U. L 198 z 23.7.2013, s. 45.	• Poważna przestępczość • Bezpieczeństwo wewnętrzne • Zwalczanie terroryzmu	• Obywatele państw trzecich	• SIS II • Europol • Interpol
------------	---	---	---	---

Eurodac	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona), Dz.U. L 180 z 29.6.2013, s. 1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca, Dz.U. L 180 z 29.6.2013, s. 31.	• Imigracja • Poważna przestępczość • Bezpieczeństwo wewnętrzne • Zwalczanie terroryzmu	• Obywatele państw trzecich	Europol
----------------	---	--	---	---------

Dane dotyczące przelotu pasażera (PNR)	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, Dz.U. L 119 z 4.5.2016, s. 132.	• Poważna przestępczość • Bezpieczeństwo wewnętrzne • Zwalczanie terroryzmu	• Obywatele UE • Obywatele państw trzecich	Europol
System danych pasażera przekazywanych przed podróżą (APIS)	Dyrektywa Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie obowiązku przekazywania przez przewoźników danych dotyczących pasażerów, Dz.U. L 261 z 6.8.2004, s. 24.	• Kontrola graniczna • Imigracja	Obywatele państw trzecich	
CIS	Decyzja Rady 2009/917/WSiSW z dnia 30 listopada 2009 r. w sprawie stosowania technologii informatycznej do potrzeb celnych, Dz.U. L 323 z 10.12.2009, s. 20.	• Zwalczanie nielegalnego handlu	• Obywatele Europy • Obywatele państw trzecich	Europol
FADO	Wspólne działanie (98/700/WSiSW) z dnia 3 grudnia 1998 r. przyjęte przez Radę na podstawie artykułu K.3 Traktatu o Unii Europejskiej, dotyczące ustanowienia Europejskiego Systemu Archiwizacji Obrazu (FADO), Dz.U. L 333 z 9.12.1998, s. 4.	• Walka z fałszowaniem dokumentów • Polityka imigracyjna • Współpraca policyjna	• Obywatele Europy • Obywatele państw trzecich	

3. PRAWODAWSTWO – KONTEKST PRAWNY, ZASADY I WSKAZÓWKI DOTYCZĄCE PODSTAWOWYCH METOD I SYSTEMÓW ŁĄCZNOŚCI

3.0. Dyrektywa o ochronie danych⁴⁶

Dyrektywa (UE) nr 2016/680, uchylająca decyzję ramową Rady 2008/977/WSiSW⁴⁷, ustanawia szczególne zasady odnoszące się do:

- ochrony osób fizycznych, bez względu na obywatelstwo czy miejsce zamieszkania, w związku z przetwarzaniem, w sposób zautomatyzowany lub niezautomatyzowany, ich danych osobowych przez policję lub inne organy ścigania dokonywanym w ramach działalności tych organów, oraz
- wymiany danych osobowych na terytorium Unii przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia postępowań przygotowawczych w ich sprawie, wykrywania ich lub ścigania, albo wykonywania kar.

Przedmiotowa dyrektywa ma na celu zapewnienie jednakowego stopnia ochrony osób fizycznych poprzez prawnie wykonalne prawa obowiązujące w całej Unii oraz zapobieganie różnicom w stosowanych praktykach utrudniającym wymianę danych osobowych między właściwymi organami.

Państwa członkowskie powinny dokonać transpozycji dyrektywy do dnia 6 maja 2018 r. Jednak w przypadkach wymagających niewspółmiernie dużego wysiłku, państwa członkowskie mogą postanowić, że – na zasadzie wyjątku i w odniesieniu do operacji wykonywanych za pośrednictwem zautomatyzowanych systemów przetwarzania utworzonych przed dniem 6 maja 2016 r. – wdrożą stosowne przepisy dotyczące monitorowania do dnia 6 maja 2023 r.

⁴⁶ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

⁴⁷ Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. L 350 z 30.12.2008, s. 60). Decyzja ramowa traci moc ze skutkiem od dnia 6 maja 2018 r.

Termin „właściwe organy” obejmuje organy publiczne, takie jak organy sądowe, policja lub inne organy ścigania, a także wszelkie inne organy lub podmioty, którym prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów wspomnianej dyrektywy. Działalność organów ścigania koncentruje się głównie na zapobieganiu przestępstwom, prowadzeniu postępowań przygotowawczych w ich sprawie, ich wykrywaniu lub ściganiu. Działania te mogą obejmować również czynności policji podczas demonstracji, dużych imprez sportowych czy zamieszek. Czynności te obejmują również utrzymywanie prawa i porządku, jako zadania powierzonego tym organom, gdy jest to konieczne do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i dla podstawowych interesów społecznych i do zapobiegania takim zagrożeniom, które mogą prowadzić do popełnienia czynu zabronionego.

Przetwarzanie danych osobowych do celów niewchodzących w zakres działań wymienionych powyżej, które to przetwarzanie państwa członkowskie mogą dodatkowo powierzyć organom ścigania, oraz przetwarzanie danych osobowych objęte prawem Unii regulowane jest przepisami rozporządzenia (UE) 2016/679⁴⁸. Ponadto dyrektywa (UE) nr 2016/680 nie obejmuje przetwarzania danych osobowych związanego z czynnościami w zakresie bezpieczeństwa narodowego, czynnościami agencji lub jednostek zajmujących się bezpieczeństwem narodowym, ani przetwarzania danych osobowych przez państwa członkowskie podczas czynności związanych ze wspólną polityką zagraniczną i bezpieczeństwa⁴⁹.

Do celów dyrektywy o ochronie danych:

- **„dane osobowe”** oznaczają wszelkie informacje dotyczące osoby fizycznej („osoba, której dane dotyczą”) zidentyfikowanej lub możliwej do zidentyfikowania, bezpośrednio lub pośrednio, w szczególności na podstawie imienia i nazwiska, numeru identyfikacyjnego, danych dotyczące lokalizacji, identyfikatora internetowego lub co najmniej jednego znaku szczególnego związanego z jej tożsamością fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną;

Państwa członkowskie zapewniają, by właściwe organy przetwarzające dane osobowe – w stosownych przypadkach i w miarę możliwości – wyraźnie rozróżniały dane osobowe poszczególnych kategorii osób, których dane dotyczą, takich jak: a) osoby podejrzane o popełnienie czynu zabronionego, b) osoby skazane za taki czyn, c) pokrzywdzeni czynem zabronionym oraz d) osoby inne w stosunku do czynu zabronionego, takie jak świadkowie.

⁴⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

⁴⁹ Tytuł V, rozdział 2 Traktatu o Unii Europejskiej (TUE).

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

Dane osobowe muszą być przetwarzane zgodnie z prawem i rzetelnie, oraz jedynie w konkretnych celach przewidzianych przez prawo. Aby takie przetwarzanie danych osobowych było zgodne z prawem, powinno ono być niezbędne do wykonania zadań realizowanych przez właściwy organ we wspomnianych powyżej celach związanych z egzekwowaniem prawa. Zasada rzetelnego przetwarzania obowiązująca w ochronie danych jest pojęciem odrębnym względem prawa do rzetelnego procesu, które jest zdefiniowane w art. 47 Karty i w art. 6 Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności. Dane osobowe muszą być adekwatne i właściwe w stosunku do celów przetwarzania.

Przetwarzanie szczególnie chronionych danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych wyłącznie w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności lub orientacji seksualnej osoby fizycznej jest dozwolone wyłącznie wtedy, jeżeli jest bezwzględnie niezbędne, podlega odpowiednim zabezpieczeniom w odniesieniu do praw i wolności osoby, której dane dotyczą, oraz odbywa się wyłącznie przy spełnieniu ściśle określonych i restrykcyjnych warunków.

Zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych jest utworzenie krajowych organów nadzorczych, które mają możliwość wykonywania swych funkcji w sposób całkowicie niezależny. Organy nadzorcze powinny monitorować stosowanie przepisów przyjętych na mocy przedmiotowej dyrektywy oraz powinny przyczyniać się do ich spójnego stosowania w całej Unii. Ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna właściwych organów krajowych i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania jasnego podziału obowiązków.

Transgraniczne przekazywanie danych osobowych może narazić na szwank możliwości osób fizycznych w zakresie prawnej ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych danych. Jednocześnie organy nadzorcze mogą uznać, że nie są w stanie rozpatrzyć skargi lub przeprowadzić postępowania w sprawie działalności, która ma miejsce poza granicami ich państwa. Ich starania na rzecz współpracy w kontekście transgranicznym mogą także zostać zakłócone przez niewystarczające uprawnienia prewencyjne lub zaradcze oraz niespójne systemy prawne. Należy więc upowszechniać ściślejszą współpracę między organami nadzorującymi ochronę danych w celu wspierania wymiany informacji z ich zagranicznymi odpowiednikami.

3.1. Szwedzka decyzja ramowa⁵⁰

Jako rozwinięcie dorobku Schengen decyzja ramowa Rady 2006/960/WSiSW („szwedzka decyzja ramowa”) ustanawia w szczególności zasady dotyczące terminów i standardowe formularze na potrzeby transgranicznej wymiany informacji⁵¹, na podstawie uprzedniego wniosku lub z własnej inicjatywy, między wyznaczonymi właściwymi organami ścigania państw członkowskich w celu:

- zapobiegania przestępstwom lub działalności przestępczej, ich wykrywania i prowadzenia dochodzeń w ich sprawie, jeżeli odpowiadają one lub są równoważne przestępstwom lub działalności przestępczej określonym w europejskim nakazie aresztowania⁵², lub
- zapobiegania bezpośredniemu i poważnemu zagrożeniu bezpieczeństwa publicznego.

Wyznaczone organy są zobowiązane do udzielenia odpowiedzi w ciągu najwyżej ośmiu godzin w pilnych przypadkach, gdy poszukiwane informacje lub dane wywiadowcze są dostępne bezpośrednio organom ścigania. Informacje nie są przekazywane, jeżeli:

- zagrożone jest bezpieczeństwo narodowe,
- mogłoby to zakłócić prowadzone w danej chwili dochodzenia,
- wniosek dotyczy przestępstwa zagrożonego zgodnie z prawem państwa członkowskiego, do którego skierowany jest wniosek, karą pozbawienia wolności na okres nie dłuższy niż jeden rok,
- właściwy organ sądowy odmówi dostępu do informacji.

⁵⁰ Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej, Dz.U. L 386 z 29.12.2006, s. 89, sprostowanie w Dz.U. L 75 z 15.3.2007, s. 26.

⁵¹ Zob. poniżej rys. 1.

⁵² 8216/2/08 REV2: Ostateczna wersja europejskiego podręcznika „Jak wystawiać europejski nakaz aresztowania”. Artykuł 2 decyzji ramowej Rady 2002/584/WSiSW w sprawie europejskiego nakazu aresztowania określa zakres takiego nakazu.

Termin „informacje lub dane wywiadowcze” obejmują następujące dwie kategorie:

- każdy rodzaj informacji lub danych będących w posiadaniu organów ścigania;
- każdy rodzaj informacji lub danych będących w posiadaniu organów publicznych lub podmiotów prywatnych, które są dostępne organom ścigania bez stosowania środków przymusu.

Zakres tych kategorii zależy od ustawodawstwa krajowego. Rodzaj informacji udostępnianych przez każde państwo członkowskie wskazano w zestawieniach informacyjnych dotyczących poszczególnych państw załączonych do niniejszego podręcznika.

Dane są udostępniane Europolowi, o ile wymieniane informacje lub dane wywiadowcze odnoszą się do przestępstw lub działalności przestępczej objętych mandatem Europolu. Informacje i dane wywiadowcze są przetwarzane zgodnie z odpowiednimi kodami postępowania Europolu. SIENA (stworzona na potrzeby Europolu aplikacja sieci bezpiecznej wymiany informacji) ułatwia wymianę informacji zgodnie ze szwedzką decyzją ramową.

Państwa członkowskie zapewniają, by warunki transgranicznej wymiany informacji nie były bardziej rygorystyczne niż warunki stosowane w przypadku wymiany wewnętrznej. Właściwe organy ścigania nie są w szczególności zobowiązane do występowania przed transgraniczną wymianą informacji o zgodę sądu ani zezwolenie, gdy poszukiwane informacje są dostępne na szczeblu krajowym bez takiej zgody lub upoważnienia. Jeżeli jednak wymagane jest upoważnienie organu sądowego, organ sądowy, wydając decyzję, stosuje w przypadku wymiany transgranicznej takie same zasady jak te, które obowiązują w przypadku sprawy wyłącznie wewnętrznej. W zestawieniach informacyjnych dotyczących poszczególnych państw wskazano, które informacje wymagają upoważnienia sądowego.

Ponieważ użytkownicy uznali standardowy formularz wniosku za zbyt skomplikowany, przygotowano nieobowiązkowy formularz wniosku o informacje lub dane wywiadowcze⁵³. Jeżeli użycie tego uproszczonego formularza jest niemożliwe, zaleca się użycie innego formularza lub tekstu opisowego w dowolnym formacie.

Jednak wnioski te muszą w każdym przypadku spełniać wymogi art. 5 szwedzkiej decyzji ramowej i zawierać przynajmniej następujące obowiązkowe elementy:

- informacje natury administracyjnej, m.in.: państwo członkowskie występujące z wnioskiem, organ występujący z wnioskiem, data, numer referencyjny lub numery referencyjne, państwo(-a) członkowskie, do którego(-ych) wystąpiono z wnioskiem,
- wskazanie, czy wymagany jest pilny tryb postępowania, a jeżeli tak – z jakiego powodu,
- opis potrzebnych informacji lub danych wywiadowczych,

⁵³ Zob. poniżej rys. 2.

- o ile są znane: tożsamość osoby (osób) lub dane identyfikacyjne przedmiotu(-ów), których dotyczy postępowanie karne lub operacja wywiadowcza w sprawie karnej stanowiące podstawę wniosku o przekazanie informacji lub danych wywiadowczych (np. opis przestępstwa lub przestępstw, okoliczności ich popełnienia itp.),
- wskazanie, w jakim celu potrzebne są informacje i dane wywiadowcze,
- związek między celem a osobą, której dotyczą informacje i dane wywiadowcze,
- przesłanki pozwalające przypuszczać, że potrzebne informacje lub dane wywiadowcze znajdują się w państwie członkowskim, do którego wystąpiono z wnioskiem,
- wszelkie ograniczenia co do użycia informacji zawartych we wniosku („kody postępowania”).

Państwo członkowskie występujące z wnioskiem może wybrać spośród wszystkich istniejących kanałów służących międzynarodowej łączności organów ścigania (SIRENE, Europol, Interpol, dwustronne punkty kontaktowe). Państwo członkowskie odpowiadające na wniosek zwykle korzysta z tego samego kanału, z którego skorzystano, by złożyć wniosek. Jeżeli jednak państwo członkowskie, do którego wystąpiono z wnioskiem, w uzasadnionych przypadkach odpowiada, korzystając z innego kanału, informuje o tej zmianie organ występujący z wnioskiem. Językiem używanym do sporządzenia wniosku i przekazania informacji jest język stosowany w obrębie użytego kanału.

Przegląd **obowiązujących umów dwustronnych lub umów innego rodzaju** załączony jest do niniejszego podręcznika.

Rysunek 1

ZAŁĄCZNIK A

WYMIANA INFORMACJI ZGODNIE Z DECYZJĄ RAMOWĄ RADY 2006/960/WSiSW FORMULARZ DO STOSOWANIA PRZEZ PAŃSTWO CZŁONKOWSKIE, DO KTÓREGO ZWRÓCONO SIĘ Z WNIOSEM, W PRZYPADKU PRZEKAZANIA INFORMACJI/OPÓŹNIENIA/ODMOWY

Niniejszego formularza używa się w celu przekazania informacji lub danych wywiadowczych, których dotyczy wniosek informowania organu składającego wniosek o niemożności dotrzymania zwykłego terminu, o konieczności przekazania wniosku do organu sądowego z prośbą o wydanie upoważnienia lub o odmowie przekazania informacji.

Niniejszy formularz może zostać wykorzystany więcej niż raz podczas trwania procedury (np. jeżeli wniosek musi najpierw zostać przekazany organowi sądowemu, zaś później okazuje się, że odmówiono jego wykonania).

Organ, do którego zwrócono się z wnioskiem (nazwa, adres, telefon, faks, e-mail, państwo członkowskie)	
Szczegółowe informacje dotyczące podmiotu obsługującego (fakultatywne):	
Numer referencyjny niniejszej odpowiedzi	
Data i numer referencyjny poprzedniej odpowiedzi	
Odpowiedź skierowana do następującego organu składającego wniosek	
Data i godzina złożenia wniosku	
Numer referencyjny wniosku	

Zwykły termin zgodnie z art. 4 decyzji ramowej 2006/960/WSiSW wynosi	
Przestępstwo podlega art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW / informacje lub dane wywiadowcze, których dotyczy wniosek, są przechowywane w bazie danych bezpośrednio dostępnej dla organu ścigania w państwie członkowskim, do którego został skierowany wniosek.	Wymaga pilnego rozpatrzenia → ☐ 8 godzin
	Nie wymaga pilnego rozpatrzenia → ☐ 1 tydzień
Pozostałe przypadki	→ ☐ 14 dni

Informacje przekazane zgodnie z decyzją ramową 2006/960/WSiSW: Przekazane informacje i dane wywiadowcze
1. Wykorzystanie przekazanych informacji lub danych wywiadowczych ☐ mogą być wykorzystywane wyłącznie do celów, w których zostały dostarczone, lub w celu zapobieżenia bezpośredniemu i poważnemu zagrożeniu bezpieczeństwa publicznego; ☐ zezwala się wykorzystać również do innych celów, z zastrzeżeniem spełnienia następujących warunków (fakultatywne):
2. Wiarygodność źródła informacji ☐ wiarygodne ☐ raczej wiarygodne ☐ niewiarygodne ☐ niemożliwe do oceny
3. Dokładność informacji lub danych wywiadowczych ☐ pewne ☐ ustalone przez źródło ☐ pogłoski - potwierdzone ☐ pogłoski - niepotwierdzone

4. Wyniki dochodzenia lub operacji wywiadowczej, podczas których doszło do wymiany informacji, należy przekazać organowi przesyłającemu.

- ☐ tak
☐ nie

5. W przypadku spontanicznej wymiany, przyczyny, dla których uznano, że informacje lub dane wywiadowcze mogłyby pomóc w wykryciu przestępstw, o których mowa w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW, w zapobieganiu tym przestępstwom lub w dochodzeniu:

OPÓŹNIENIE - niemożliwe jest udzielenie odpowiedzi w zwykłym terminie zgodnie z art. 4 decyzji ramowej 2006/960/WSiSW

Informacja lub dane wywiadowcze nie mogą być przekazane w wyznaczonym terminie z następującego powodu.....

Jest prawdopodobne, że odpowiedź zostanie udzielona w ciągu:

- ☐ 1 dnia ☐ 2 dni ☐ 3 dni
☐ tygodni(a)
☐ 1 miesiąca

- ☐ Zwrócono się o upoważnienie do organu sądowego.
Przewidywany czas trwania procedury prowadzącej do wydania/odmowy upoważnienia wynosi tygodni.

ODMOWA - Informacja lub dane wywiadowcze

- (☐)nie mogły być dostarczone i wymagane na szczeblu krajowym lub
(☐)nie mogą być dostarczone z jednego lub więcej poniższych powodów:

A - Przyczyna związana z nadzorem sądowym, który uniemożliwia przekazanie lub wymaga zastosowania wzajemnej pomocy prawnej

- ☐ właściwy organ sądowy nie wydał upoważnienia do dostępu i wymiany informacji lub danych wywiadowczych
- ☐ informacje lub dane wywiadowcze, których dotyczy wnioski, zostały uprzednio uzyskane poprzez zastosowanie środków przymusu i ich przekazanie jest niedozwolone zgodnie z prawem krajowym
- ☐ informacje lub dane wywiadowcze nie znajdują się w posiadaniu
- organów ścigania; lub
 - organów publicznych lub podmiotów prywatnych w sposób, który umożliwia organom ścigania dostęp do nich bez stosowania środków przymusu
- ☐ B - przekazanie informacji lub danych wywiadowczych, których dotyczy wnioski, mogłoby zagrozić istotnym interesom bezpieczeństwa narodowego lub powodzeniu trwającego dochodzenia karnego, operacji wywiadowczej lub bezpieczeństwu osób, lub byłoby w wyraźny sposób nieproporcjonalne lub bez znaczenia dla celów, dla jakich wnioskowano o ich przekazanie.

W przypadkach A lub B należy przestawić, o ile uznano to za konieczne, dodatkowe informacje lub przyczyny odmowy (fakultatywne):

- ☐ D - Organ, do którego zwrócono się z wnioskiem, podjął decyzję o odmowie wykonania, gdyż zgodnie z prawem państwa członkowskiego, do którego został skierowany wniosek, wniosek dotyczy następującego przestępstwa (należy określić charakter przestępstwa i jego skutki prawne), które pociąga za sobą karę pozbawienia wolności na okres do 1 roku.
- ☐ E - informacje lub dane wywiadowcze, których dotyczy wnioski, nie są dostępne
- ☐ F - informacje lub dane wywiadowcze, których dotyczy wnioski, zostały uzyskane od innego państwa członkowskiego lub państwa trzeciego i podlegają zasadzie szczególności, zaś państwo członkowskie lub państwo trzecie, które je udostępniło, nie wyraziło zgody na dalsze przekazanie tych informacji lub danych wywiadowczych.

ZAŁĄCZNIK B

WYMIANA INFORMACJI ZGODNIE Z DECYZJĄ RAMOWĄ RADY 2006/960/WSiSW FORMULARZ WNIOSKU
O UDOSTĘPNIENIE INFORMACJI I DANYCH WYWIADOWCZYCH DO STOSOWANIA PRZEZ PAŃSTWO
CZŁONKOWSKIE SKŁADAJĄCE WNIOSEK

Niniejszy formularz stosuje się przy składaniu wniosku o udostępnienie informacji i danych wywiadowczych zgodnie z decyzją ramową 2006/960/WSiSW.

I – Dane administracyjne

Organ składający wniosek (nazwa, adres, telefon, faks, e-mail, państwo członkowskie)	
Szczegółowe informacje dotyczące podmiotu obsługującego (fakultatywne):	
Zwraca się do następującego państwa członkowskiego:	
Data i godzina złożenia niniejszego wniosku:	
Numer referencyjny wniosku:	

Poprzednie wnioski

☐ Jest to pierwszy wniosek w tej sprawie

☐ Jest to kolejny wniosek w tej samej sprawie

Poprzedni(e) wniosek(wnioski)			Odpowiedź(odpowiedzi)	
	Data	Numer referencyjny (w państwie członkowskim składającym wniosek)	Data	Numer referencyjny (w państwie członkowskim, do którego skierowano wniosek)
1.				
2.				
3.				
4.				

Jeżeli wniosek został skierowany do więcej niż jednego organu w państwie członkowskim, do którego został złożony wniosek, proszę podać, jakich użyto kanałów:

☐ Europejskie jednostki narodowe (ENU)/Oficer łącznikowy Europolu

☐ Do wiadomości
☐ Do wykonania

☐ Interpol NCB

☐ Do wiadomości
☐ Do wykonania

☐ Sirene

☐ Do wiadomości
☐ Do wykonania

☐ Oficer łącznikowy

☐ Do wiadomości
☐ Do wykonania

☐ Inne (jakie?):

☐ Do wiadomości
☐ Do wykonania

Jeżeli ten sam wniosek przesłano do innych państw członkowskich, proszę podać to(te) państwo(-a) członkowskie oraz jakich użyto kanałów (fakultatywne)

II – Terminy

Przypomnienie: terminy zgodnie z art. 4 decyzji ramowej 2006/960/WSiSW

A – Przepięstwo podlega art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW

i

informacje lub dane wywiadowcze, których dotyczy wniosek, sã przechowywane w bazie danych bezpośrednio dostępczej dla organu ścigania

→ Wniosek wymaga pilnego rozpatrzenia → Termin: 8 godzin z możliwością przedłużenia

→ Wniosek nie wymaga pilnego rozpatrzenia → Termin: 1 tydzień

B - Inne przypadki: Termin: 14 dni

☐ WYMAGA pilnego rozpatrzenia
☐ NIE WYMAGA PILNEGO ROZPATRZENIA
Podstawa do pilnego rozpatrzenia (np. podejrzani sã przetrzymywani w areszcie, sprawa musi znaleźć się w sądzie przed konkretną datą):
Informacje lub dane wywiadowcze, których dotyczy wniosek

RODZAJ PRZESTĘPSTW(A) LUB DZIAŁALNOŚCI PRZESTĘPCZEJ(-YCH) STANOWIĄCYCH PRZEDMIOT DOCHODZENIA
Opis okoliczności, w jakich zostało(-y) popełnione przestępstwo(-a), w tym czas, miejsce i stopień uczestnictwa w przestępstwie(-ach) osoby, której dotyczy wniosek o udostępnienie informacji lub danych wywiadowczych:

Charakter przestępstw(a)																																	
A - zastosowanie art. 4 ust. 1 lub 3 decyzji ramowej 2006/960/WSiSW ☐ A.1. Przestępstwo podlega w państwie członkowskim składającym wniosek karze pozbawienia wolności na maksymalny okres nie krótszy niż trzy lata ORAZ A.2. Przestępstwo stanowi jedno lub kilka spośród następujących czynów: <table border="0"> <tr> <td>☐ udział w organizacji przestępczej</td> <td>☐ pranie dochodów z przestępstwa</td> </tr> <tr> <td>☐ terroryzm</td> <td>☐ fałszowanie pieniędzy, w tym euro</td> </tr> <tr> <td>☐ handel ludźmi</td> <td>☐ cyberprzestępczość</td> </tr> <tr> <td>☐ seksualne wykorzystywanie dzieci i pornografia dziecięca</td> <td>☐ przestępstwa przeciwko środowisku naturalnemu, w tym nielegalny obrót zagrożonymi gatunkami zwierząt i roślin oraz ich odmianami</td> </tr> <tr> <td>☐ nielegalny obrót środkami odurzającymi i psychotropowymi</td> <td>☐ udzielanie pomocy w nielegalnym przekroczeniu granicy lub pobycie</td> </tr> <tr> <td>☐ nielegalny obrót bronią, amunicją i materiałami wybuchowymi</td> <td>☐ zabójstwo, spowodowanie ciężkiego uszczerbku na zdrowiu</td> </tr> <tr> <td>☐ korupcja</td> <td>☐ nielegalny obrót organami i tkankami ludzkimi</td> </tr> <tr> <td>☐ oszustwa, w tym oszustwa na szkodę interesów finansowych Wspólnot Europejskich w rozumieniu Konwencji z dnia 26 lipca 1995 r. w sprawie ochrony interesów finansowych Wspólnot Europejskich</td> <td>☐ uprowadzenie osoby, bezprawne pozbawienie wolności i wzięcie zakładników</td> </tr> <tr> <td>☐ kradzież w formie zorganizowanej rozbój z użyciem broni</td> <td>☐ rasizm i ksenofobia</td> </tr> <tr> <td>☐ nielegalny obrót dobrami kultury, w tym antykami i dziełami sztuki</td> <td>☐ nielegalny obrót materiałami jądrowymi i radioaktywnymi</td> </tr> <tr> <td>☐ sprzeniewierzenie cudzego mienia</td> <td>☐ obrót kradzionymi pojazdami</td> </tr> <tr> <td>☐ wymuszenie rozbójnicze</td> <td>☐ zgwałcenie</td> </tr> <tr> <td>☐ podrabianie i piractwo produktów</td> <td>☐ podpalenie</td> </tr> <tr> <td>☐ fałszowanie dokumentów urzędowych i obrót takimi dokumentami</td> <td>☐ przestępstwa należące do właściwości Międzynarodowego Trybunału Karnego</td> </tr> <tr> <td>☐ fałszowanie środków płatniczych</td> <td>☐ porwanie statku wodnego lub powietrznego</td> </tr> <tr> <td>☐ nielegalny obrót hormonami i innymi substancjami wzrostu</td> <td>☐ sabotaż</td> </tr> </table> → Z tego powodu przestępstwo podlega art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW. Odnośnie do terminów udzielenia odpowiedzi na niniejszy wniosek stosuje się art. 4 ust. 1 (przypadki pilne) oraz art. 4 ust. 3 (przypadki niewymagające pilnego rozpatrzenia) decyzji ramowej 2006/960/WSiSW		☐ udział w organizacji przestępczej	☐ pranie dochodów z przestępstwa	☐ terroryzm	☐ fałszowanie pieniędzy, w tym euro	☐ handel ludźmi	☐ cyberprzestępczość	☐ seksualne wykorzystywanie dzieci i pornografia dziecięca	☐ przestępstwa przeciwko środowisku naturalnemu, w tym nielegalny obrót zagrożonymi gatunkami zwierząt i roślin oraz ich odmianami	☐ nielegalny obrót środkami odurzającymi i psychotropowymi	☐ udzielanie pomocy w nielegalnym przekroczeniu granicy lub pobycie	☐ nielegalny obrót bronią, amunicją i materiałami wybuchowymi	☐ zabójstwo, spowodowanie ciężkiego uszczerbku na zdrowiu	☐ korupcja	☐ nielegalny obrót organami i tkankami ludzkimi	☐ oszustwa, w tym oszustwa na szkodę interesów finansowych Wspólnot Europejskich w rozumieniu Konwencji z dnia 26 lipca 1995 r. w sprawie ochrony interesów finansowych Wspólnot Europejskich	☐ uprowadzenie osoby, bezprawne pozbawienie wolności i wzięcie zakładników	☐ kradzież w formie zorganizowanej rozbój z użyciem broni	☐ rasizm i ksenofobia	☐ nielegalny obrót dobrami kultury, w tym antykami i dziełami sztuki	☐ nielegalny obrót materiałami jądrowymi i radioaktywnymi	☐ sprzeniewierzenie cudzego mienia	☐ obrót kradzionymi pojazdami	☐ wymuszenie rozbójnicze	☐ zgwałcenie	☐ podrabianie i piractwo produktów	☐ podpalenie	☐ fałszowanie dokumentów urzędowych i obrót takimi dokumentami	☐ przestępstwa należące do właściwości Międzynarodowego Trybunału Karnego	☐ fałszowanie środków płatniczych	☐ porwanie statku wodnego lub powietrznego	☐ nielegalny obrót hormonami i innymi substancjami wzrostu	☐ sabotaż
☐ udział w organizacji przestępczej	☐ pranie dochodów z przestępstwa																																
☐ terroryzm	☐ fałszowanie pieniędzy, w tym euro																																
☐ handel ludźmi	☐ cyberprzestępczość																																
☐ seksualne wykorzystywanie dzieci i pornografia dziecięca	☐ przestępstwa przeciwko środowisku naturalnemu, w tym nielegalny obrót zagrożonymi gatunkami zwierząt i roślin oraz ich odmianami																																
☐ nielegalny obrót środkami odurzającymi i psychotropowymi	☐ udzielanie pomocy w nielegalnym przekroczeniu granicy lub pobycie																																
☐ nielegalny obrót bronią, amunicją i materiałami wybuchowymi	☐ zabójstwo, spowodowanie ciężkiego uszczerbku na zdrowiu																																
☐ korupcja	☐ nielegalny obrót organami i tkankami ludzkimi																																
☐ oszustwa, w tym oszustwa na szkodę interesów finansowych Wspólnot Europejskich w rozumieniu Konwencji z dnia 26 lipca 1995 r. w sprawie ochrony interesów finansowych Wspólnot Europejskich	☐ uprowadzenie osoby, bezprawne pozbawienie wolności i wzięcie zakładników																																
☐ kradzież w formie zorganizowanej rozbój z użyciem broni	☐ rasizm i ksenofobia																																
☐ nielegalny obrót dobrami kultury, w tym antykami i dziełami sztuki	☐ nielegalny obrót materiałami jądrowymi i radioaktywnymi																																
☐ sprzeniewierzenie cudzego mienia	☐ obrót kradzionymi pojazdami																																
☐ wymuszenie rozbójnicze	☐ zgwałcenie																																
☐ podrabianie i piractwo produktów	☐ podpalenie																																
☐ fałszowanie dokumentów urzędowych i obrót takimi dokumentami	☐ przestępstwa należące do właściwości Międzynarodowego Trybunału Karnego																																
☐ fałszowanie środków płatniczych	☐ porwanie statku wodnego lub powietrznego																																
☐ nielegalny obrót hormonami i innymi substancjami wzrostu	☐ sabotaż																																
☐ B - przestępstwo(-a) nie zostało(-y) ujęte w A. W tym przypadku należy podać opis przestępstw(a):																																	
Cel, w jakim składa się wniosek o udostępnienie informacji lub danych wywiadowczych																																	
Związek pomiędzy celem, w jakim składa się wniosek o udostępnienie informacji lub danych wywiadowczych, a osobą, której one dotyczą																																	
Tożsamość(ci) (o ile jest(sa) znana(-e)) osoby/osób, w sprawie której(-ych) prowadzone jest dochodzenie karne lub operacja wywiadowcza dotycząca przestępstwa, będące podstawą wniosku o udostępnienie informacji lub danych wywiadowczych																																	
Przyczyny pozwalające przypuszczać, że informacje lub dane wywiadowcze, których dotyczy wniosek, znajdują się w państwie członkowskim, do którego zwrócono się z wnioskiem																																	
Ograniczenia dotyczące wykorzystania informacji zawartej w niniejszym wniosku do celów innych niż te, dla jakich zostały dostarczone lub w celu zapobieżenia bezpośredniemu i poważnemu zagrożeniu bezpieczeństwa publicznego																																	
☐ zezwolenie na wykorzystanie udzielone ☐ zezwolenie na wykorzystanie udzielone, ale nie podawać źródła informacji ☐ nie wykorzystywać bez upoważnienia udzielonego przez źródło informacji ☐ nie wykorzystywać																																	

WNIOSEK O UDOSTĘPNIENIE INFORMACJI I DANYCH WYWIADOWCZYCH

zgodnie z decyzją ramową Rady 2006/960/WSiSW

I - Dane administracyjne

Państwo członkowskie występujące z wnioskiem:	
Organ występujący z wnioskiem (nazwa, adres, telefon, faks, adres poczty elektronicznej):	
Szczegółowe informacje dotyczące podmiotu zajmującego się sprawą (<i>fakultatywnie</i>):	
Data i godzina złożenia wniosku:	
Numer referencyjny wniosku:	
Poprzednie numery referencyjne:	

Państwo(-a) członkowskie, do którego(-ych) wystąpiono z wnioskiem:		
Kanał		
☐ Krajowa jednostka Europolu/Oficer łącznikowy Europolu	☐ Do wiadomości	☐ Do wykonania
☐ Krajowe biuro Interpolu	☐ Do wiadomości	☐ Do wykonania
☐ SIRENE	☐ Do wiadomości	☐ Do wykonania
☐ Oficer łącznikowy	☐ Do wiadomości	☐ Do wykonania
☐ Inny (należy podać, jaki):	☐ Do wiadomości	☐ Do wykonania

II – Pilny tryb postępowania

Wymaga pilnego rozpatrzenia:	☐ Tak ☐ Nie
Podstawa konieczności pilnego rozpatrzenia (np.: podejrzani przebywają w areszcie, sprawa musi znaleźć się w sądzie przed konkretną datą):	
<u>Zastosowanie artykułu:</u>	
Przestępstwo podlega art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW w sprawie europejskiego nakazu aresztowania:	☐ Tak ☐ Nie

III – Cel

Rodzaj przestępstw(-a) lub działalności przestępczej(-ych) stanowiących przedmiot dochodzenia
Opis: - okoliczności, w jakich zostało(-y) popełnione przestępstwo(-a) (np. czas, miejsce i charakter uczestnictwa w przestępstwie(-ach) osoby, której dotyczy wniosek o udostępnienie informacji lub danych wywiadowczych) - przesłanki pozwalające przypuszczać, że potrzebne informacje lub dane wywiadowcze znajdują się w państwie członkowskim, do którego wystąpiono z wnioskiem, - związek pomiędzy celem, w jakim wystąpiono z wnioskiem o udostępnienie informacji lub danych wywiadowczych, a osobą, której one dotyczą
☐ wniosek o wykorzystanie uzyskanych informacji jako materiału dowodowego, jeżeli jest to dopuszczalne na mocy prawa krajowego (<i>fakultatywnie</i>)

IV – Rodzaj informacji

Tożsamość (o ile jest znana) osoby (osób) lub opis przedmiotu(-ów)		
Osoba	Przedmiot(-y)	
Nazwisko:	Numer seryjny broni:	
Nazwisko rodowe:	Numer dokumentu:	
Imię:	Inny numer identyfikacyjny lub nazwa:	
Data urodzenia:	Numer rejestracyjny pojazdu:	
Miejsce urodzenia:	Numer identyfikacyjny pojazdu (VIN):	
Płeć: ☐ mężczyzna ☐ kobieta ☐ nieznana	Rodzaj dokumentów:	
Obywatelstwo:	Dane kontaktowe przedsiębiorstwa (nr telefonu, adres poczty elektronicznej, adres, strona internetowa itp.):	
Informacje dodatkowe:	Informacje dodatkowe:	
Informacje lub dane wywiadowcze, których dotyczy wnioski		
Osoba	Pojazd	Inne
☐ sprawdzenie tożsamości ☐ przeszukanie baz danych ☐ wyszukanie adresu/miejsca pobytu	☐ uzupełnienie danych identyfikacyjnych ☐ ustalenie tożsamości właściciela ☐ ustalenie tożsamości kierowcy ☐ przeszukanie baz danych	☐ ustalenie, o jakie przedsiębiorstwo chodzi ☐ wyszukanie informacji o przedsiębiorstwie w bazach danych ☐ wyszukanie dokumentów w bazach danych ☐ ustalenie numeru telefonu / faksu ☐ ustalenie właściciela adresu poczty elektronicznej ☐ wyszukanie adresu ☐ wyszukanie broni
Inne:		

V – Kody postępowania

Ograniczenia dotyczące wykorzystania informacji zawartych w niniejszym wniosku do celów innych niż te, dla jakich zostały dostarczone, lub w celu zapobieżenia bezpośredniemu i poważnemu zagrożeniu bezpieczeństwa publicznego

☐ do wykorzystania wyłącznie przez policję, nie można wykorzystać w postępowaniu sądowym

☐ przed wykorzystaniem należy skontaktować się z podmiotem udzielającym informacji

3.2. Schengen – wymiana danych w SIS II i poza tym systemem

Układ z Schengen podpisany 14 czerwca 1985 r. został uzupełniony w 1990 r. przez Konwencję wykonawczą do układu z Schengen (CISA)⁵⁴, na mocy której utworzono strefę Schengen poprzez zniesienie kontroli granicznych pomiędzy państwami strefy Schengen i wprowadzenie wspólnych przepisów dotyczących wiz oraz współpracę policyjną i sądową. Konwencja wykonawcza do układu z Schengen ustanawia ogólny wymóg dotyczący współpracy policyjnej i uprawnia organy policji do wymiany informacji w granicach dozwolonych w ich krajowych systemach prawnych.

Wraz z wejściem w życie Traktatu z Amsterdamu w 1999 r. środki współpracy dotychczas objęte ramami Schengen włączono do ram prawnych Unii Europejskiej, a kwestie związane z Schengen są obecnie regulowane przez organy prawodawcze UE. Protokół w sprawie dorobku Schengen załączony do Traktatu z Amsterdamu ustanawia szczegółowe warunki tego procesu integracji.

System informacyjny Schengen (SIS) został ustanowiony na mocy tytułu IV konwencji z 19 czerwca 1990 r. Stanowi on zasadniczy instrument stosowania postanowień dorobku Schengen. Jest również środkiem mającym kompensować brak kontroli osób na granicach wewnętrznych w obrębie strefy Schengen poprzez zastosowanie narzędzia pozwalającego na wymianę informacji między właściwymi organami.

To, że na ramy prawne regulujące SIS składają się obecnie dwa odrębne instrumenty, tj. rozporządzenie odnoszące się do korzystania z SIS na granicach oraz decyzja Rady odnosząca się do współpracy policyjnej, nie zmienia faktu, że SIS stanowi jeden system informacyjny.

⁵⁴ Konwencja wykonawcza do układu z Schengen z dnia 14 czerwca 1985 roku między rządami Państw Unii Gospodarczej Beneluxu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, Dz.U. L 239 z 22.9.2000, s. 19.

Prawodawstwo

Rozporządzenie (WE) 987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz.U. L 381 z 28.12.2006, s. 4.

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.

Podstawowe przepisy

System informacyjny Schengen (SIS) jest zarówno systemem współpracy policyjnej, jak i systemem kontroli granicznej i wspiera współpracę operacyjną organów policji i organów sądowiczych w sprawach karnych. Z SIS korzystać mogą wyznaczeni funkcjonariusze policji, straży granicznej i służb celnych oraz organy wizowe i sądowicze w całej strefie Schengen⁵⁵.

System informacyjny Schengen drugiej generacji („SIS II”) działa obecnie w 26 państwach członkowskich UE oraz w czterech państwach niebędących członkami UE, które zostały włączone we współpracę Schengen: Norwegii, Islandii, Szwajcarii i Liechtensteinie.

- Jeśli chodzi o współpracę policyjną, to zarówno Zjednoczone Królestwo, jak i Irlandia zwróciły się z wnioskiem o umożliwienie im brania w niej udziału, ale zgodę na to, by – tymczasowo i w ramach pierwszego kroku pozwalającego na przeprowadzenie oceny przed ostateczną decyzją o „wprowadzeniu w życie” – pozyskiwać w czasie rzeczywistym dane z tej części SIS⁵⁶ uzyskało, w roku 2015, jedynie Zjednoczone Królestwo. Zjednoczone Królestwo ani Irlandia nie uczestniczą w stosowaniu SIS do celów kontroli granicznej.

⁵⁵ Skonsolidowany wykaz właściwych organów krajowych, w którym dla każdego organu podaje się, jakie dane może przeszukiwać i do jakich celów, jest corocznie publikowany w *Dzienniku Urzędowym Unii Europejskiej* na mocy art. 31 ust. 8 rozporządzenia w sprawie SIS i art. 46 ust. 8 decyzji w sprawie SIS II.

⁵⁶ Decyzja wykonawcza Rady (UE) 2015/215 z dnia 10 lutego 2015 r. w sprawie wprowadzenia w życie przepisów dorobku Schengen dotyczących ochrony danych oraz tymczasowego wprowadzenia w życie części przepisów dorobku Schengen dotyczących Systemu Informacyjnego Schengen w odniesieniu do Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej, Dz.U. L 36 z 12.2.2015, s. 8.

- Bułgaria, Rumunia⁵⁷ i Chorwacja⁵⁸ stosują przepisy dorobku Schengen dotyczące współpracy policyjnej i kontroli granicznej. Uzyskały one dostęp do danych w SIS w czasie rzeczywistym, po to by można było ocenić, czy prawidłowo stosują one przepisy dorobku Schengen odnoszące się do SIS. Po uzyskaniu prawidłowego wyniku oceny, w odrębnych decyzjach Rady ustalona zostanie data zniesienia kontroli na granicach wewnętrznych. Do tego czasu nadal obowiązują pewne ograniczenia w korzystaniu z SIS.
- Cypr nie ma jeszcze dostępu do SIS.

Dane SIS II można wyszukiwać online (pod warunkiem spełnienia restrykcyjnych warunków w zakresie ochrony danych) całodobowo w biurach SIRENE, w punktach kontroli granicznej, na terytorium kraju i w konsulatach za granicą. Dane są określane terminem „wpisy”, przy czym przez wpis rozumie się zestaw danych, które umożliwiają organom zidentyfikowanie **osób**, tj. obywateli europejskich i obywateli państw spoza UE, lub **przedmiotów** z myślą o podjęciu stosownych działań w celu zwalczania przestępczości i imigracji nieuregulowanej.

Specjalnie upoważniony personel Europolu ma, w granicach swojego mandatu, prawo bezpośredniego dostępu i wyszukiwania danych wprowadzonych do SIS II i może występować o dodatkowe informacje od danego państwa członkowskiego.

Krajowi przedstawiciele oddelegowani do Eurojustu oraz ich asystenci mają, w granicach swojego mandatu, prawo dostępu do danych wprowadzonych do SIS II i ich wyszukiwania.

Zgodnie z art. 47 CISA oficerowie łącznikowi oddelegowani do organów policyjnych w innych państwach strefy Schengen lub państwach trzecich są odpowiedzialni za wymianę informacji na mocy:

- artykułu 39 ust. 1, 2 i 3 zgodnie z prawem krajowym do celów zapobiegania przestępstwom i ich wykrywania;
- artykułu 46, nawet z własnej inicjatywy, do celów zapobiegania przestępstwom przeciwko porządkowi i bezpieczeństwu publicznemu lub zapobiegania zagrożeniom dla porządku i bezpieczeństwa publicznego.

⁵⁷ Decyzja Rady 2010/365/UE z dnia 29 czerwca 2010 r. w sprawie stosowania w Republice Bułgarii i w Rumunii przepisów dorobku Schengen związanych z systemem informacyjnym Schengen, Dz.U. L 166 z 1.7.2010, s. 17.

⁵⁸ Decyzja Rady (UE) 2017/733 z dnia 25 kwietnia 2017 r. w sprawie stosowania w Republice Chorwacji przepisów dorobku Schengen dotyczących Systemu Informacyjnego Schengen, Dz.U. L 108 z 26.4.2017, s. 31.

Należy zauważyć, że przepisy art. 39 ust. 1, 2 i 3 oraz art. 46, w zakresie w jakim odnoszą się do wymiany informacji i danych wywiadowczych dotyczących poważnej przestępczości, zastępuje się przepisami decyzji ramowej Rady 2006/960/WSiSW, tj. szwedzkiej decyzji ramowej. Jednak przepisy art. 39 ust. 1, 2 i 3 oraz art. 46 nadal obowiązują w odniesieniu do przestępstw podlegających karze pozbawienia wolności do 12 miesięcy.

3.3. Europol

Prawodawstwo

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. 53–114 (mające zastosowanie od 1 maja 2017 r.).

Podstawowe przepisy

Celem Europolu jest wspieranie i zwiększanie skuteczności działań właściwych organów państw członkowskich odpowiedzialnych za zapobieganie przestępstwom i ich zwalczanie, jak również ich wzajemnej współpracy w zapobieganiu przestępczości zorganizowanej, terroryzmowi i innym formom poważnej przestępczości i zwalczaniu tych zjawisk, gdy dotyczą one co najmniej dwóch państw członkowskich. W tym celu Europol gromadzi, przechowuje, przetwarza, analizuje i wymienia informacje i dane wywiadowcze dotyczące przestępstw.

Każde państwo członkowskie wyznacza jednostkę krajową (ENU) działającą jako organ pośredniczący w kontaktach między Europolem a właściwymi organami państw członkowskich. Jednostka krajowa wykonuje zadania związane z wymianą istotnych informacji i danych wywiadowczych. Każda jednostka krajowa oddelegowuje co najmniej jednego oficera łącznikowego, który ma pełnić funkcje krajowego biura łącznikowego przy Europolu i reprezentować interesy danej jednostki krajowej. Oficerowie łącznikowi powołani są do wymiany informacji między państwami członkowskimi a Europolem, a z drugiej strony – do dwustronnej wymiany z innymi państwami. Takie dwustronne wymiany informacji mogą dotyczyć spraw wykraczających poza mandat Europolu.

Rozporządzenie w sprawie Europolu wprowadza nową koncepcję przetwarzania danych, która jest często nazywana „koncepcją zintegrowanego zarządzania danymi”. Koncepcję zintegrowanego zarządzania danymi można zdefiniować jako możliwość wykorzystywania informacji związanych z przestępstwem na potrzeby wielu działań, wskazanych przez właściciela danych, co pozwala na zarządzanie tymi danymi i ich przetwarzanie w sposób zintegrowany, neutralny pod względem technologicznym. Na mocy decyzji Rady w sprawie Europolu przetwarzanie danych zostało tak pomyślane, by to poszczególne systemy stanowiły jego trzon. Rozporządzenie w sprawie Europolu nie zawiera już odniesień do systemów, ale w zamian wymaga wskazania celów przetwarzania. Aby użytkownicy mogli płynnie przechodzić na tę drugą metodę działania, mogą nadal korzystać z istniejących systemów, ale muszą z nimi pracować w sposób zgodny z nowymi ramami prawnymi.

Jednostka krajowa jest odpowiedzialna za łączność z systemem informacyjnym Europolu (EIS) wykorzystywanym do przetwarzania danych niezbędnych do wykonywania zadań Europolu. Jednostka krajowa, oficerowie łącznikowi i należycie umocowani pracownicy Europolu mają prawo do wprowadzania danych do systemów i pobierania z nich danych. Informacje wprowadzone do EIS uznaje się generalnie za przekazane do celów sprawdzania krzyżowego (art. 18 ust. 2 lit. a) rozporządzenia) i do celów analiz strategicznych/tematycznych (art. 18 ust. 2 lit. b) rozporządzenia).

3.4. Interpol

Prawodawstwo

Konstytucja Interpolu⁵⁹

Zasady przetwarzania informacji⁶⁰

Zasady kontroli informacji i dostępu do akt Interpolu

Podstawowe przepisy

Zadaniem Interpolu jest ułatwianie międzynarodowej współpracy policyjnej w celu zapobiegania przestępczości i jej zwalczania dzięki ściślejszej współpracy i innowacji w zakresie kwestii policyjnych i bezpieczeństwa. Działania są podejmowane w granicach przepisów obowiązujących w państwach będących członkami oraz w duchu Powszechnej deklaracji praw człowieka.

W każdym ze 190 państw członkowskich funkcjonuje krajowe biuro Interpolu zatrudniające własnych dobrze wyszkolonych funkcjonariuszy organów ścigania.

Konstytucja Interpolu jest umową międzynarodową, która potwierdza, że członkami są rządy wszystkich państw, które uczestniczyły w jej przyjęciu w 1956 r., i ustanawia procedurę składania wniosków o przyjęcie do Interpolu dla państw, które nie były członkami w 1956 r.

Jako główny dokument prawny konstytucja określa cele i założenia Interpolu. Ustanawia mandat organizacji, który polega na zapewnieniu jak najszerzej współpracy wszystkich organów policji kryminalnej i zmniejszeniu liczby przestępstw prawa powszechnego.

Oprócz konstytucji ramy prawne Interpolu tworzą pewne teksty stanowiące podstawę jego działania. W celu zapewnienia zgodności z przepisami wprowadzono różne poziomy kontroli. Dotyczą one kontroli przeprowadzanych przez krajowe biura Interpolu, przez Sekretariat Generalny i przez niezależny organ monitorujący znany jako Komisja Kontroli Akt Interpolu.

⁵⁹ <http://www.interpol.int/en/About-INTERPOL/Legal-materials/The-Constitution>

⁶⁰ <http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts>

3.5. Oficerowie łącznikowi

Prawodawstwo

Konwencja wykonawcza do układu z Schengen z dnia 19 czerwca 1990 r. (CISA)⁶¹, art. 47

Decyzja Rady 2003/170/WSiSW z dnia 27 lutego 2003 r. w sprawie wspólnego wykorzystywania oficerów łącznikowych oddelegowanych za granicę przez organy ścigania państw członkowskich⁶²,

Decyzja Rady 2006/560/WSiSW z dnia 24 lipca 2006 r. zmieniająca decyzję 2003/170/WSiSW w sprawie wspólnego wykorzystywania oficerów łącznikowych oddelegowanych za granicę przez organy ścigania państw członkowskich⁶³

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. 53–114 (mające zastosowanie od 1 maja 2017 r.)

Decyzja Rady 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz.U. L 210 z 6.8.2008, s. 1.

Umowy dwustronne

⁶¹ Konwencja wykonawcza do układu z Schengen z dnia 19 czerwca 1990 r. (CISA), Dz.U. L 239 z 22.9.2000, s. 19.

⁶² Decyzja Rady 2003/170/WSiSW z dnia 27 lutego 2003 r., Dz.U. L 67 z 12.3.2003, s. 27.

⁶³ Decyzja Rady 2006/560/WSiSW z dnia 24 lipca 2006 r., Dz.U. L 219 z 10.8.2006, s. 31.

Podstawowe przepisy

Zgodnie z art. 47 CISA państwa członkowskie „mogą zawierać umowy dwustronne przewidujące oddelegowanie, na czas określony lub nieokreślony, oficerów łącznikowych z jednego państwa [członkowskiego] do organów policji innego państwa [członkowskiego]”. Oficerowie łącznikowi nie są uprawnieni do wykonywania żadnych czynności policyjnych samodzielnie, a art. 47 stanowi, że takie oddelegowania „mają na celu udoskonalenie i przyspieszenie współpracy, szczególnie poprzez okazywanie pomocy:

- a) w postaci wymiany informacji do celów zwalczania przestępstw zarówno poprzez zapobieganie im, jak i ich ściganie;
- b) przy wykonywaniu wniosków o wzajemną pomoc oraz pomoc sądową w sprawach karnych;
- c) w zadaniach wykonywanych przez organy odpowiedzialne za nadzorowanie granicy zewnętrznej.

Więcej informacji na temat takiego delegowania pracowników można znaleźć w dokumencie „Zbiór zaleceń związanych z meczami piłki nożnej”⁶⁴ i w zaleceniu Rady z dnia 6 grudnia 2007 r. w sprawie Podręcznika współpracy podczas ważnych imprez międzynarodowych przeznaczonego dla policji i organów bezpieczeństwa⁶⁵.

Postanowienie CISA, zgodnie z którym krajowi oficerowie łącznikowi mogą również reprezentować interesy jednego lub większej liczby państw członkowskich, został doprecyzowany decyzją Rady w sprawie wspólnego wykorzystywania oficerów łącznikowych oddelegowanych za granicę przez organy ścigania państw członkowskich (zmieniona w 2006 r.). Przewidziano również usprawnienie współpracy między oficerami łącznikowymi w różnych państwach członkowskich w ich miejscu oddelegowania. Na różnych forach podkreślano, że należy zachęcać do takiej współpracy.

⁶⁴ Rezolucja Rady z dnia 3 czerwca 2010 r. w sprawie zaktualizowanego podręcznika z zaleceniami w zakresie międzynarodowej współpracy policyjnej oraz w zakresie działań prewencyjnych i kontrolnych związanych z aktami przemocy i zakłóceniami porządku podczas międzynarodowych meczów piłki nożnej, które dotyczą co najmniej jednego państwa członkowskiego, Dz.U. C 165 z 24.6.2010, s. 1.

⁶⁵ Dz.U. C 314 z 22.12.2007, s. 4.

Zgodnie z rozporządzeniem w sprawie Europolu każde państwo członkowskie wyznacza jednostkę krajową, która działa jako organ pośredniczący w kontaktach między Europolem a właściwymi organami państw członkowskich odpowiedzialnymi za zapobieganie przestępstwom i ich zwalczanie. Jednostka krajowa wykonuje zadania związane z wymianą istotnych informacji i danych wywiadowczych. Każda jednostka krajowa oddelegowuje co najmniej jednego oficera łącznikowego, który ma pełnić funkcje krajowego biura łącznikowego przy Europolu i reprezentować interesy danej jednostki krajowej. Oficerowie łącznikowi powołani są do wymiany informacji między jednostką krajową a Europolem, a z drugiej strony – do dwustronnej wymiany informacji między innymi jednostkami krajowymi. Takie dwustronne wymiany informacji mogą dotyczyć spraw wykraczających poza mandat Europolu.

Decyzja Rady 2008/615/WSiSW („decyzja z Prüm”) przewiduje w art. 17 i 18 oddelegowywanie funkcjonariuszy krajowych do celów ochrony porządku i bezpieczeństwa publicznego oraz prewencji kryminalnej.

3.6. Wymiana danych na mocy decyzji z Prüm

Prawodawstwo

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

Podstawowe przepisy

Państwa członkowskie udzielają sobie na zasadzie wzajemności transgranicznego dostępu online do danych referencyjnych w wyznaczonych krajowych zbiorach analiz DNA oraz do automatycznych systemów identyfikacji daktyloskopijnej (AFIS) i do danych rejestracyjnych pojazdów (zob. rozdz. 2 decyzji Rady 2008/615/WSiSW).

W każdym państwie członkowskim należy wyznaczyć krajowe punkty kontaktowe. Przepisy dotyczące ochrony danych i bezpieczeństwa danych muszą być odpowiednio wyjaśnione w ustawodawstwie krajowym. Zautomatyzowane porównywanie anonimowych profili biometrycznych jest oparte na systemie trafieniowym (figuruje / nie figuruje), z wyjątkiem danych rejestracyjnych pojazdów, gdzie wyszukiwane dane właściciela/posiadacza są podawane automatycznie.

W przypadku dopasowania danych biometrycznych krajowy punkt kontaktowy państwa członkowskiego wyszukujące dane otrzymuje w sposób automatyczny dane referencyjne, z którymi stwierdzono zgodność.

Następnie, korzystając z procedur wzajemnej pomocy, w tym tych przyjętych na mocy szwedzkiej decyzji ramowej, można wystąpić o dodatkowe szczegółowe dane osobowe oraz inne informacje dotyczące danych referencyjnych.

Przekazanie takich danych uzupełniających podlega prawu krajowemu, w tym przepisom o pomocy prawnej, państwa członkowskiego, do którego wystąpiono z wnioskiem. Uznaje się, że przekazanie danych osobowych wymaga zapewnienia odpowiedniego poziomu ochrony danych przez państwo członkowskie je otrzymujące⁶⁶.

W celu zapobiegania przestępstwom, a także w celu ochrony porządku i bezpieczeństwa publicznego w przypadku dużych imprez mających wymiar transgraniczny państwa członkowskie mogą, zarówno na wniosek, jak i z własnej inicjatywy, przekazywać sobie dane nieosobowe i osobowe. W tym celu wyznacza się specjalne krajowe punkty kontaktowe (zob. rozdział 3 decyzji Rady 2008/615/WSiSW).

By zapobiegać przestępstwom terrorystycznym, w pewnych okolicznościach państwa członkowskie mogą dostarczać sobie dane osobowe. W tym celu wyznacza się specjalne krajowe punkty kontaktowe (zob. rozdział 4 decyzji Rady 2008/615/WSiSW).

⁶⁶ Decyzja Rady 2008/615/WSiSW respektuje poziom ochrony przetwarzania danych osobowych określony w Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, w protokole dodatkowym do tej konwencji z dnia 8 listopada 2001 r., oraz w wymogach zalecenia nr R (87) 15 Rady Europy w sprawie wykorzystania danych osobowych przez policję.

3.7. Wizowy system informacyjny (VIS)

Prawodawstwo

Decyzja Rady z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS) (2004/512/WE), Dz.U. L 213 z 15.6.2004, s. 5.

Decyzja Rady 2013/392/UE dotycząca wyznaczenia daty, od której staje się skuteczna decyzja 2008/633/WSiSW w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do wizowego systemu informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania, Dz.U. L 198 z 23.7.2013, s. 45

Podstawowe przepisy

VIS jest systemem, który umożliwia właściwym organom krajowym wprowadzanie i uaktualnianie danych wizowych oraz korzystanie z tych danych drogą elektroniczną. Jest on oparty na architekturze scentralizowanej i składa się z centralnego systemu informacyjnego, centralnego wizowego systemu informacyjnego (CS-VIS), interfejsu krajowego w każdym państwie członkowskim (NI-VIS), oraz infrastruktury łączności między CS-VIS i NI-VIS.

16 kwietnia 2015 r. Trybunał Sprawiedliwości Unii Europejskiej unieważnił decyzję Rady 2013/392/UE z dnia 22 lipca 2013 r. dotyczącą wyznaczenia daty, od której staje się skuteczna decyzja 2008/633/WSiSW w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do wizowego systemu informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania. Jednocześnie Trybunał orzekł, że skutki decyzji 2013/392 zostają utrzymane do czasu wejścia w życie nowego aktu, który ją zastąpi.

3.8. Eurodac

Prawodawstwo

Europejski zautomatyzowany system identyfikacji odcisków palców (Eurodac) to system komputerowy pierwotnie zaprojektowany, by ułatwić skuteczne stosowanie konwencji dublińskiej. Konwencja dublińska, podpisana 15 czerwca 1990 r., zastąpiona została rozporządzeniem Rady (WE) nr 343/2003 z dnia 18 lutego 2003 r. ustanawiającym kryteria i mechanizmy określania państwa członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z państw członkowskich przez obywatela państwa trzeciego.

W związku ze zmianami w rozporządzeniach w sprawie Eurodac sporządzono ich wersję przekształconą –

rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona) (Dz.U. L 180 z 29.6.2013, s. 1).

Podstawowe przepisy

Rozporządzenie nr 603/2013 formułuje cel Eurodac i określa warunki dostępu wyznaczonych krajowych organów ścigania i Europolu do danych Eurodac na potrzeby zapobiegania przestępstwom terrorystycznym⁶⁷ oraz innym poważnym przestępstwom kryminalnym⁶⁸, ich wykrywania lub prowadzenia dochodzeń w ich sprawie.

⁶⁷ Decyzja ramowa Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. L 164 z 22.6.2002, s. 3).

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

3.9. Konwencja neapolitańska II

Prawodawstwo

Akt Rady z dnia 18 grudnia 1997 r. ustanawiający na podstawie artykułu K.3 Traktatu o Unii Europejskiej Konwencję w sprawie pomocy wzajemnej i współpracy między administracjami celnymi, opublikowany w Dz.U. C 24 z 23.1.1998, s. 1.

Podstawowe przepisy

Państwa członkowskie udzielają sobie pomocy w celu zapobiegania naruszeniom krajowych przepisów celnych i wykrywania ich oraz ścigania i karania naruszeń wspólnotowych i krajowych przepisów celnych. W ramach dochodzeń w sprawach karnych konwencja neapolitańska II ustanawia procedury, dzięki którym administracje celne mogą współdziałać oraz wymieniać, z własnej inicjatywy lub na wniosek, dane dotyczące nielegalnego handlu.

Wnioski składa się w formie pisemnej w języku urzędowym państwa członkowskiego, w którym znajduje się organ będący adresatem wniosku, lub w języku akceptowanym przez ten organ. Istnieje formularz określający standard przekazywania informacji. Właściwe organy przekazują wszystkie informacje, które mogą pomóc w zapobieganiu naruszeniom oraz ich wykrywaniu i ściganiu. Wymieniają one między sobą dane osobowe, czyli wszelkie informacje dotyczące osoby fizycznej, która jest zidentyfikowana lub możliwa do zidentyfikowania.

Organ będący adresatem wniosku lub powiadomiony przez niego właściwy organ, udzielając pomocy, postępuje tak, jakby działał na swoją rzecz lub na wniosek innego organu swojego państwa członkowskiego.

3.9.1. System informacji celnej – CIS⁶⁹

System informacji celnej stanowi uzupełnienie konwencji neapolitańskiej II⁷⁰. Scentralizowany system informacyjny jest zarządzany przez Komisję i ma na celu usprawnienie administracji celnych państw członkowskich dzięki szybkiej wymianie informacji z myślą o zapobieganiu poważnym naruszeniom przepisów prawa krajowego i wspólnotowego, prowadzeniu dochodzeń w ich sprawie i ich ścigania. CIS umożliwia również ustanowienie identyfikującej bazy danych rejestru celnego (FIDE), która ma ułatwiać prowadzenie dochodzeń celnych.

Organy wyznaczone przez państwa członkowskie⁷¹ mają bezpośredni dostęp do danych zawartych w CIS. W celu zwiększenia komplementarności z Europolem i Eurojustem oba te organy mają dostęp do danych CIS i FIDE w trybie do odczytu.

CIS zawiera dane osobowe w odniesieniu do towarów, środków transportu, przedsiębiorstw, osób i wyrobów, a także środków pieniężnych, zatrzymanych, zajętych lub skonfiskowanych. Dane osobowe mogą być kopiowane z CIS do innych systemów przetwarzania danych wyłącznie w związku z zarządzaniem ryzykiem lub analizami operacyjnymi, do których mają dostęp jedynie analitycy wyznaczeni przez państwa członkowskie.

FIDE umożliwia organom krajowym odpowiedzialnym za prowadzenie dochodzeń celnych określenie – w momencie wszczynania dochodzenia – innych organów, które mogły prowadzić dochodzenia w sprawie danej osoby lub przedsiębiorstwa.

⁶⁹ Decyzja Rady 2009/917/WSiSW z dnia 30 listopada 2009 r. w sprawie stosowania technologii informatycznej do potrzeb celnych, Dz.U. L 323 z 10.12.2009, s. 20.

⁷⁰ Konwencja sporządzona na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie pomocy wzajemnej i współpracy między administracjami celnymi, Dz.U. C 24 z 23.1.1998, s. 2.

⁷¹ Wdrożenie art. 7 ust. 2 i art. 8 ust. 3 decyzji Rady 2009/917/WSiSW z dnia 30 listopada 2009 r. w sprawie stosowania technologii informatycznej do potrzeb celnych – zaktualizowany wykaz właściwych organów, 13394/11 ENFOCUSTOM 85.

3.10. Biura ds. odzyskiwania mienia (ARO) i CARIN

Prawodawstwo

Decyzja Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotycząca współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem, Dz.U. L 332 z 18.12.2007, s. 103.

Międzyagencyjna Sieć Odzyskiwania Mienia Camden (CARIN) została ustanowiona w Hadze 22–23 września 2004 r. przez Austrię, Belgię, Niderlandy, Irlandię, Niemcy i Zjednoczone Królestwo.

Podstawowe przepisy

W związku z przyjęciem decyzji Rady 2007/845/WSiSW⁷² wszystkie państwa członkowskie ustanowiły i wyznaczyły biura ds. odzyskiwania mienia (ARO). Biura te mogą bezpośrednio wymieniać informacje w sprawach dotyczących odzyskiwania aktywów za pośrednictwem systemu SIENA. Pod auspicjami Komisji Europejskiej i Europolu sieć ARO ułatwia współpracę pomiędzy biurami państw członkowskich ds. odzyskiwania mienia i strategiczną dyskusję oraz wymianę optymalnych rozwiązań. Będący częścią Europolu urząd ds. mienia pochodzącego z działalności przestępczej (Criminal Assets Bureau – ECAB) działa jako centralny punkt kontaktowy do spraw odzyskiwania mienia w UE.

Przepisy określone w dyrektywie Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej⁷³ przyczynią się do zwiększenia skuteczności współpracy między biurami ds. odzyskiwania mienia w Unii Europejskiej. Państwa członkowskie wezwano do dokonania transpozycji dyrektywy do 4 października 2016 r.

⁷² Decyzja Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotycząca współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem, Dz.U. L 332 z 18.12.2007, s. 103.

⁷³ Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej, Dz.U. L 127 z 29.4.2014, s. 39.

Międzyagencyjna Sieć Odzyskiwania Mienia Camden (CARIN), ustanowiona w 2004 r., by wspierać transgraniczną identyfikację, zamrażanie, zajmowanie i konfiskatę mienia związanego z przestępstwem, zwiększa wymianę informacji dotyczących różnych krajowych strategii wykraczającą poza UE.

Sieć CARIN obejmuje specjalistów z 53 jurysdykcji i dziewięciu organizacji międzynarodowych, którzy działają jako punkty kontaktowe do celów szybkiej transgranicznej wymiany informacji na żądanie lub z własnej inicjatywy (stan na 2015 r.). Krajowe biura ds. odzyskiwania mienia współpracują ze sobą lub z innymi organami, ułatwiając ustalanie pochodzenia i identyfikację korzyści pochodzących z przestępstwa. Chociaż wszystkie państwa członkowskie utworzyły biura ds. odzyskiwania mienia, istnieją duże różnice między państwami członkowskimi, jeżeli chodzi o strukturę organizacyjną, zasoby i działania tych jednostek.

Informacje uzyskane w ramach wymiany mogą być wykorzystywane zgodnie z przepisami o ochronie danych otrzymującego je państwa członkowskiego oraz podlegają takim samym przepisom o ochronie danych, jak gdyby zostały pozyskane w otrzymującym je państwie członkowskim. Należy propagować spontaniczną wymianę informacji zgodnie z tą decyzją, z zastosowaniem procedur i terminów przewidzianych w szwedzkiej decyzji ramowej.

3.11. Jednostki analityki finansowej (FIU)

Prawodawstwo

Decyzja Rady 2000/642/WSiSW z dnia 17 października 2000 r. dotycząca uzgodnień w sprawie współpracy pomiędzy jednostkami wywiadu finansowego państw członkowskich w odniesieniu do wymiany informacji

Dz.U. L 271 z 24.10.2000, s. 4.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 658/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE

Dz.U. L 141 z 5.6.2015, s. 73.

Podstawowe przepisy

Wniosek musi określać sposób, w jaki zostaną wykorzystane otrzymane informacje, a odpowiadająca jednostka FIU zobowiązana jest do dostarczenia wszystkich stosownych informacji, w tym informacji finansowych oraz danych dotyczących egzekwowania prawa; stanowi to kluczowy element decyzji. Jednak jednostka analityki finansowej może odmówić ujawnienia informacji, jeżeli miałyby to zakłócić toczące się w sprawie karnej dochodzenie lub byłyby wyraźnie nieproporcjonalne do uzasadnionych interesów danej osoby, której dotyczą dane, lub gdyby w inny sposób byłyby to niezgodne z podstawowymi zasadami prawa krajowego.

Jednostki analityki finansowej podejmują wszelkie niezbędne działania, łącznie ze środkami bezpieczeństwa, w celu zapewnienia, aby przekazana informacja nie została udostępniona innym organom, agencjom lub jednostkom. Państwa członkowskie zapewniają właściwe i chronione kanały łączności pomiędzy jednostkami FIU i przyjmują uzgodnienia w tej sprawie.

FIU.NET to zdecentralizowana sieć komputerowa służąca wymianie informacji między FIU.

FIU.NET, początkowo zaprojektowana, by wzmocnić pozycję jednostek FIU, rozwinęła się w ostatnich latach i z bezpiecznego podstawowego narzędzia do uporządkowanej dwustronnej wymiany informacji przekształciła się w bezpieczne wielofunkcyjne narzędzie wielostronnej wymiany informacji, obejmujące elementy zarządzania sprawami oraz półautomatyczną standaryzację procesów. W FIU.NET każdy nowy element i zautomatyzowany proces są fakultatywne, a jednostki nie są zobowiązane do ich stosowania. Poszczególne jednostki analityki finansowej mogą podjąć decyzję, z jakich możliwości i elementów udostępnianych w ramach FIU.NET korzystają. Wykorzystują jedynie te elementy, które im odpowiadają, wyłączając te, których nie potrzebują lub których nie chcą.

3.12. Umowa między UE a USA w sprawie programu śledzenia środków należących do terrorystów (system TFTP)

Prawodawstwo

Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu z Unii Europejskiej do Stanów Zjednoczonych danych z komunikatów finansowych do celów Programu śledzenia środków finansowych należących do terrorystów

Dz.U. L 195 z 27.7.2010.

Podstawowe przepisy

Po atakach terrorystycznych 11 września UE i Stany Zjednoczone postanowiły blisko współpracować i zawarły umowę w sprawie przetwarzania i przekazywania danych z komunikatów finansowych przez Unię Europejską Stanom Zjednoczonym do celów programu śledzenia środków finansowych należących do terrorystów (umowa UE–USA w sprawie TFTP). Zgodnie z tą umową Departament Skarbu USA również udostępnia informacje TFTP organom ścigania, bezpieczeństwa publicznego lub zwalczania terroryzmu danych państw członkowskich, a w stosownych przypadkach Europolowi i Eurojustowi.

System TFTP jest wyposażony w rozbudowane środki kontroli w celu zapewnienia, by wszystkie gwarancje, w tym te dotyczące ochrony danych osobowych, były przestrzegane. Dane przetwarzane są wyłącznie na potrzeby zapobiegania terroryzmowi lub jego finansowaniu, dochodzenia w tych sprawach, wykrywania lub ścigania takich zjawisk.

Na potrzeby tej umowy Departament Skarbu USA może się zwracać do wyznaczonych dostawców międzynarodowych usług w zakresie komunikatów finansowych dotyczących płatności o udostępnienie danych z komunikatów finansowych dotyczących płatności oraz danych powiązanych przechowywanych na terytorium UE.

Korzystanie z danych TFTP przez państwa członkowskie, Europol i Eurojust jest ograniczone faktem, że analiza płatności transgranicznych w ramach TFTP opiera się wyłącznie na wiadomościach FIN (transfer między instytucjami finansowymi) – wiadomościach typu SWIFT, dzięki którym informacje finansowe są przekazywane z jednej instytucji finansowej do drugiej. Nie są rozpatrywane inne sposoby dokonywania płatności. Jednak system TFTP jest jedynym mechanizmem umożliwiającym, w krótkim czasie, mapowanie i profilowanie transakcji, w odniesieniu do których istnieje podejrzenie związku z terroryzmem lub finansowaniem terroryzmu, do celów zwiększenia bezpieczeństwa wewnętrznego.

Dzięki większej wiedzy na temat klauzul wzajemności przewidzianych w tej umowie organy UE w coraz większym stopniu stosują ten mechanizm, by korzystać z wymiany danych z USA. Należy w tym kontekście zauważyć, że wszystkie wnioski złożone przez organy UE i dotyczące wyszukiwania w systemie TFTP muszą spełniać wymogi art. 10 umowy.

Chociaż umowa nie przewiduje, by z wnioskiem o wyszukiwanie stosownych informacji otrzymanych w ramach programu TFTP państwa członkowskie zwracały się za pośrednictwem Europolu, przydatne byłoby, by – w celu poprawy reakcji UE na terroryzm i jego finansowanie – państwa członkowskie przynajmniej informowały Europol, w sposób systematyczny i we właściwym czasie, o swoich bezpośrednich wnioskach składanych na mocy art. 10. Aby ułatwić państwom członkowskim kierowanie wniosków o wyszukiwanie w systemie TFTP, Europol utworzył pojedynczy punkt kontaktowy (SPOC), co w połączeniu ze środowiskiem pliku roboczego do celów analizy i dobrze ugruntowaną współpracą z Departamentem Skarbu umożliwia mu skuteczne rozpatrywanie wniosków państw członkowskich.

3.13. Wymiana informacji pochodzących z rejestrów karnych (ECRIS)

Prawodawstwo

Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji, Dz.U. L 93 z 7.4.2009, s. 23. Ta decyzja ramowa uchyla decyzję Rady 2005/876/WSiSW z dnia 21 listopada 2005 r. w sprawie wymiany informacji pochodzących z rejestru karnego, Dz.U. L 322 z 9.12.2005, s. 33.

Decyzja Rady 2009/316/WSiSW w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), zgodnie z art. 11 decyzji ramowej 2009/315/WSiSW, opiera się na zasadach ustanowionych w decyzji ramowej 2009/315/WSiSW oraz wdraża i uzupełnia te zasady z technicznego punktu widzenia.

Podstawowe przepisy

Decyzja ramowa Rady 2009/315/WSiSW zobowiązuje skazujące państwo członkowskie do jak najszybszego przekazania wszelkich wyroków skazujących wpisanych do rejestru karnego państwu(-om) członkowskiemu(-im), którego(-ych) dana osoba jest obywatelem, jak również wszelkich zmian lub skreśleń dokonanych w tym wyroku. Państwo członkowskie obywatelstwa ma obowiązek przechowywać te informacje do celów dalszego przekazania, a wszelkie zmiany lub skreślenia dokonane w skazującym państwie członkowskim skutkują taką samą zmianą lub skreśleniem w rejestrze karnym państwa, którego obywatele jest skazany. Gdy państwo członkowskie obywatelstwa występuje o informacje o wyroku do potrzeb postępowania karnego, państwo członkowskie, do którego wystąpiono z wnioskiem, jest zobowiązane do przekazania informacji o wyrokach skazujących zapisanych w rejestrze karnym. Jeżeli przekazanie informacji wymagane jest do celów innych niż postępowanie karne, państwo członkowskie, do którego wystąpiono z wnioskiem, odpowiada zgodnie z prawem krajowym.

Decyzja Rady 2009/316/WSiSW określa, w jaki sposób państwo członkowskie ma przekazać takie informacje. W decyzji Rady określono ramy dotyczące skomputeryzowanego systemu wymiany informacji pochodzących z rejestrów karnych. Organy centralne każdego państwa członkowskiego korzystają ze specjalnych formularzy wniosku i odpowiedzi załączonych do decyzji ramowej i z drogi elektronicznej, opisanej w tej decyzji.

3.14. Zatrzymywanie danych telekomunikacyjnych

Prawodawstwo

Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE⁷⁴.

⁷⁴ Trybunał Sprawiedliwości Unii Europejskiej wyrokiem z dnia 8 kwietnia 2014 r. uznał dyrektywę za nieważną.

Podstawowe przepisy

Dyrektywa ma zastosowanie do dostawców usług łączności elektronicznej. Dyrektywa stanowi, że dostawcy powinni zatrzymywać dane o ruchu i dotyczące lokalizacji oraz odnośne dane potrzebne do zidentyfikowania abonenta lub użytkownika, w celu przekazywania tych danych właściwym organom krajowym na ich wniosek. Do celów prowadzenia dochodzeń w sprawie poważnej przestępczości, jej wykrywania i ścigania państwa członkowskie nakładają na dostawców usług łączności elektronicznej lub publiczne sieci łączności obowiązek zatrzymywania kategorii danych niezbędnych do określenia:

- źródła połączenia,
- odbiorcy połączenia,
- daty, godziny i czasu trwania połączenia,
- rodzaju połączenia,
- narzędzia komunikacji lub tego, co może służyć za narzędzie komunikacji,
- lokalizacji urządzenia łączności ruchomej.

Nie wolno zatrzymywać danych, które ujawniają treść komunikatu.

3.15. Dyrektywa w sprawie danych PNR (danych dotyczących przelotu pasażera)

Prawodawstwo

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

Podstawowe przepisy

Dyrektywa ta ustanawia na poziomie unijnym wspólne ramy prawne określające przekazywanie i przetwarzanie danych PNR i określa:

- b) przekazywanie przez przewoźników lotniczych⁷⁵ danych dotyczących przelotu pasażera (zwanymi dalej „danymi PNR”), które dotyczą pasażerów lotów pozaunijnych. Jeżeli państwo członkowskie podejmie decyzję o stosowaniu dyrektywy do lotów wewnątrzunijnych, wszystkie jej przepisy stosuje się do lotów wewnątrzunijnych, tak jakby były one lotami pozaunijnymi;
- c) przetwarzanie danych PNR, w tym ich zbieranie, wykorzystywanie i zatrzymywanie przez państwa członkowskie oraz wymianę tych danych między państwami członkowskimi.

W celu przetwarzania danych PNR każde państwo członkowskie ustanawia lub wyznacza organ właściwy do pełnienia roli jednostki do spraw informacji o pasażerach (JIP). Dwa państwa członkowskie lub większa ich liczba mogą ustanowić lub wyznaczyć jeden organ jako swój wspólny JIP.

⁷⁵ Nie wpływa ona na możliwość ustanowienia przez państwa członkowskie, na mocy przepisów krajowych, systemu zbierania i przetwarzania danych PNR przekazywanych przez podmioty gospodarcze niebędące przewoźnikami, takie jak biura podróży i organizatorzy wycieczek świadczący usługi związane z podróżowaniem, w tym rezerwację lotów, na potrzeby których zbierają i przetwarzają dane PNR, lub przez dostawców usług transportowych innych niż dostawcy określani w tej dyrektywie, pod warunkiem że takie przepisy krajowe są zgodne z prawem Unii.

Dane PNR wymienione w załączniku I przedmiotowej dyrektywy są przekazywane przez przewoźników lotniczych do JIP w zakresie, w jakim już je zbierają w ramach swojej normalnej działalności. Niektórzy przewoźnicy lotniczy zatrzymują dane pasażera przekazywane przed podróżą (API) jako część danych PNR, a inni tego nie robią. Niezależnie od sposobu, w jaki przewoźnicy lotniczy gromadzą dane API, muszą je przekazać do JIP, gdzie zostaną przetworzone w taki sam sposób, jak dane PNR. Załącznik II do dyrektywy zawiera wykaz „poważnych przestępstw” wchodzących w zakres tego aktu.

Przetwarzanie danych PNR służy sprawdzeniu pasażerów przed ich planowanym przylotem do państwa członkowskiego lub odlotem z niego w celu identyfikacji osób, które wymagają dalszego sprawdzenia przez właściwe organy oraz, w stosownych przypadkach, przez Europol – w granicach jego kompetencji i na potrzeby realizowanych przez niego zadań, w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

By dokonać takiego sprawdzenia, JIP może:

- a) porównywać dane PNR z bazami danych, które mają znaczenie dla zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, w tym z bazami danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem – zgodnie z przepisami unijnymi, międzynarodowymi i krajowymi mającymi zastosowanie do takich baz danych; lub
- b) przetwarzać dane PNR według wcześniej ustalonych kryteriów.

Na szczeblu krajowym JIP przekazują dane PNR lub wyniki ich przetwarzania właściwym krajowym organom ścigania uprawnionym do dalszego zbadania sprawy lub do podjęcia odpowiednich działań w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. Choć JIP stanowią główny kanał transgranicznej wymiany informacji, w nagłych przypadkach i gdy spełnione są szczegółowo określone warunki właściwe organy mogą zwracać się bezpośrednio do JIP innego państwa członkowskiego.

Na szczeblu unijnym JIP wymieniają się między sobą zarówno danymi PNR zabranymi od przewoźników lotniczych, jak i wynikami takiego przetwarzania; Europol również uczestniczy w tej wymianie, gdyż jest uprawniony – w granicach jego kompetencji i na potrzeby realizowanych przez niego zadań – do występowania o udostępnienie przez JIP takich danych.

Dane PNR mają być zatrzymywane w bazie danych JIP przez okres pięciu lat od przekazania ich z państwa członkowskiego przylotu lub odlotu. Jednak po upływie 6 miesięcy wszystkie dane PNR zostają poddane depersonalizacji. Dokonuje się tego poprzez maskowanie tych elementów danych, które mogłyby posłużyć do bezpośredniego zidentyfikowania pasażera, którego dane dotyczą. W dyrektywie zawarto wykaz danych PNR, które podlegają maskowaniu. Po pięciu lat dane PNR są usuwane, chyba że zostały przekazane właściwemu organowi do celów zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania; w takim przypadku ich zatrzymywanie regulowane jest regulowane przez prawo krajowe.

Zgodnie z unijnym prawodawstwem dotyczącym ochrony danych dyrektywa dotycząca danych PNR zabrania przetwarzania chronionych danych osobowych, takich jak rasa czy pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne czy orientacja seksualna danej osoby.

3.16. System danych pasażera przekazywanych przed podróżą (APIS)

Prawodawstwo

Dyrektywa Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie obowiązku przekazywania przez przewoźników danych dotyczących pasażerów

Podstawowe przepisy

Dyrektywa ta ma na celu polepszenie kontroli granicznej i zwalczanie nielegalnej imigracji. W tym celu nakłada na państwa członkowskie obowiązek ustanowienia zobowiązania dla przewoźników lotniczych do przesyłania pewnych informacji dotyczących obsługiwanych przez nich podróżnych, zanim wjadą oni na terytorium Unii Europejskiej. Informacje te określa się mianem danych pasażera przekazywanych przed podróżą (API). W pewnych okolicznościach i pod pewnymi warunkami państwa członkowskie mogą również wykorzystać dane API do celów egzekwowania prawa.

Informacje takie przekazywane są na wniosek organów odpowiedzialnych za przeprowadzanie kontroli osób na granicach zewnętrznych UE.

Przewoźnicy lotniczy powinni przekazywać dane API drogą elektroniczną, lub, w przypadku gdy takie przekazanie nie powiedzie się, za pośrednictwem innych odpowiednim środków organom przeprowadzającym kontrolę graniczną w miejscu, w którym pasażerowie wjeżdżają na terytorium UE. Dane API są sprawdzane poprzez porównanie z informacjami znajdującymi się w krajowych i europejskich bazach danych, takich jak System Informacyjny Schengen (SIS) i wizowy system informacyjny (VIS).

Jeśli dane API generują trafienie w bazie danych, policja graniczna otrzymuje odpowiednie powiadomienie, a dany pasażer zostaje wyznaczony do kontroli po przybyciu.

Zgromadzone i przekazane dane API muszą zostać usunięte przez przewoźników i organy w ciągu 24 godzin od ich przekazania lub przyjazdu pasażera. Jednak służby graniczne mogą zatrzymać dane zapisane na pliku tymczasowym przez okres dłuższy niż 24 godziny, jeśli dane te są później potrzebne do celów wypełnienia funkcji statutowych organów granicznych lub do celu stosowania przepisów ustawowych i wykonawczych dotyczących wjazdu i imigracji, w tym przepisy dotyczące ochrony porządku publicznego i bezpieczeństwa narodowego.

3.17. Przestępstwa lub wykroczenia związane z bezpieczeństwem ruchu drogowego

Prawodawstwo

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/413 z dnia 11 marca 2015 r. w sprawie ułatwień w zakresie transgranicznej wymiany informacji dotyczących przestępstw lub wykroczeń przeciwko bezpieczeństwu ruchu drogowego, Dz.U. L 68, s. 9.

Podstawowe przepisy

Państwa członkowskie przyznają sobie nawzajem dostęp online do swoich krajowych danych rejestracyjnych pojazdów w celu egzekwowania kar za niektóre przestępstwa związane z bezpieczeństwem ruchu drogowego z udziałem pojazdu zarejestrowanego w państwie członkowskim innym niż państwo członkowskie, w którym miało miejsce przestępstwo lub wykroczenie. Państwo członkowskie popełnienia przestępstwa lub wykroczenia wykorzystuje uzyskane dane w celu ustalenia, kto ponosi odpowiedzialność za przestępstwo lub wykroczenie w ruchu drogowym. Wymiana informacji odnosi się do:

- przekroczenia dopuszczalnej prędkości;
- niekorzystania z pasów bezpieczeństwa;
- niezastosowania się do czerwonego sygnału świetlnego;
- kierowania pojazdem pod wpływem alkoholu;
- kierowania pojazdem pod wpływem środków odurzających;
- niedopełnienia obowiązku używania w czasie jazdy hełmów ochronnych;
- korzystania z niedozwolonego pasa ruchu;
- niezgodnego z prawem korzystania z telefonu komórkowego lub innych środków łączności podczas kierowania pojazdem.

Przy użyciu specjalnej aplikacji EUCARIS państwa członkowskie – na zasadzie wzajemności – udzielają swoim wyznaczonym krajowym punktom kontaktowym dostępu do danych rejestracyjnych pojazdów i umożliwiają im zautomatyzowane wyszukiwanie:

- a) danych pojazdów oraz
- b) danych dotyczących właścicieli lub posiadaczy pojazdu.