

Bruxelles, 4 iulie 2017
(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

NOTĂ

Sursă:	Președinția
Destinatar:	Grupul de lucru pentru schimbul de informații și protecția datelor (DAPIX)
Nr. doc. ant.:	11800/1/16 REV 1
Subiect:	Manual privind schimbul de informații în materie de aplicare a legii

1. Introducere

Manualul privind schimbul de informații în materie de aplicare a legii vizează completarea Manualului privind operațiile transfrontaliere (documentul 10505/4/09 REV4). Atât conținutul și structura manualului, cât și fișele naționale au fost aprobate de DAPIX în cadrul Strategiei de gestionare a informațiilor (SGI) pentru securitatea internă a UE cu scopul de a sprijini, de a simplifica și de a facilita schimbul transfrontalier de informații.

Pentru a spori valoarea practică a manualului, se vor pune la dispoziție traduceri în toate limbile oficiale ale Uniunii. De asemenea, manualul va fi actualizat de două ori pe an, în funcție de necesități, din perspectiva noii legislații sau a experienței practice. Versiunea actuală ține seama în special de Regulamentul Europol și de datele de contact. Aceste date de contact sunt actualizate periodic de statele membre și prevăzute în fișele naționale, care vor fi de acum emise ca addendum la manual.

2. Scopul manualului

Manualul este conceput în primul rând ca instrument pentru polițiștii care lucrează în domeniul relațiilor internaționale și, în special, pentru așa-numiții **operatori „SPOC”**. În consecință, manualul ar trebui să fie cât mai ușor de utilizat și cât mai cuprinzător cu putință.

Manualul are drept scop să informeze și să faciliteze **cooperarea practică zilnică** dintre diferitele autorități ale statelor membre implicate în schimbul de informații polițienești atât la nivel național, cât și la nivel internațional, să folosească în scopuri de formare și să asigure faptul că se vor lua decizii în mai bună cunoștință de cauză în ceea ce privește solicitarea și schimbul de informații la nivel transfrontalier.

Manualul conține **o prezentare generală a tuturor sistemelor din UE, a temeiurilor juridice și a instrumentelor în materie de schimb de informații** disponibile pentru autoritățile de aplicare a legii din statele membre. În acest mod, utilizatorul este pe deplin informat cu privire la opțiunile disponibile în momentul luării unei decizii cu privire la modalitatea de a solicita sau de a furniza informații la nivel transfrontalier.

În cele din urmă, **fișele naționale** din addendum completează manualul prin menționarea datelor de contact și a informațiilor pertinente disponibile pentru schimbul transfrontalier. Prin actualizarea periodică a acestor fișe, statele membre vor respecta numeroasele obligații de notificare asumate în temeiul diverselor instrumente. Aceste fișe naționale ar trebui să faciliteze gestionarea și găsirea informațiilor necesare.

Manualul include aceste fișe naționale, alături de informații practice esențiale cu privire la Decizia-cadru 2006/960/JAI a Consiliului („Decizia-cadru suedeză” - DCS), și înlocuiește fostele orientări DCS (documentul 9512/10 CRIMORG 90 ENFOPOL 125 ENFOCUSTOM 36 COMIX 346).

3. Conținutul manualului

Manualul este împărțit în trei părți care sunt redactate astfel încât să fie consultate separat unele de celelalte, în funcție de intenția cititorului.

Prima parte a manualului constă în **liste de verificare** care oferă o vedere de ansamblu pragmatică a opțiunilor disponibile pentru schimbul de informații și a aspectelor practice conexe. Aceste liste de verificare contribuie la orientarea utilizatorilor către punctul de contact corespunzător pentru schimbul de informații pe baza listelor de sisteme și metode disponibile în următoarele contexte operaționale principale:

- prevenirea și investigarea infracțiunilor (și a imigrației ilegale)
- combaterea terorismului
- menținerea ordinii publice și a securității

În al doilea rând, o prezentare **generală** prezintă atât organismele naționale implicate în schimbul de informații, cât și instrumentele utilizate pentru schimbul de informații. Manualul face trimitere la rolul central al Deciziei-cadru 2006/960/JAI a Consiliului („Decizia-cadru suedeză”) și al Deciziei 2008/615/JAI a Consiliului („Decizia Prüm”) în cadrul sferei mai largi a schimbului de informații la nivelul UE. Cu toate acestea, manualul nu se limitează la aceste instrumente.

În sfârșit, manualul este completat de o compilație constând în **fișe naționale** pentru fiecare stat membru, cu **detalii practice privind punctele de contact** relevante pentru schimbul transfrontalier de informații.

4. Calea de urmat

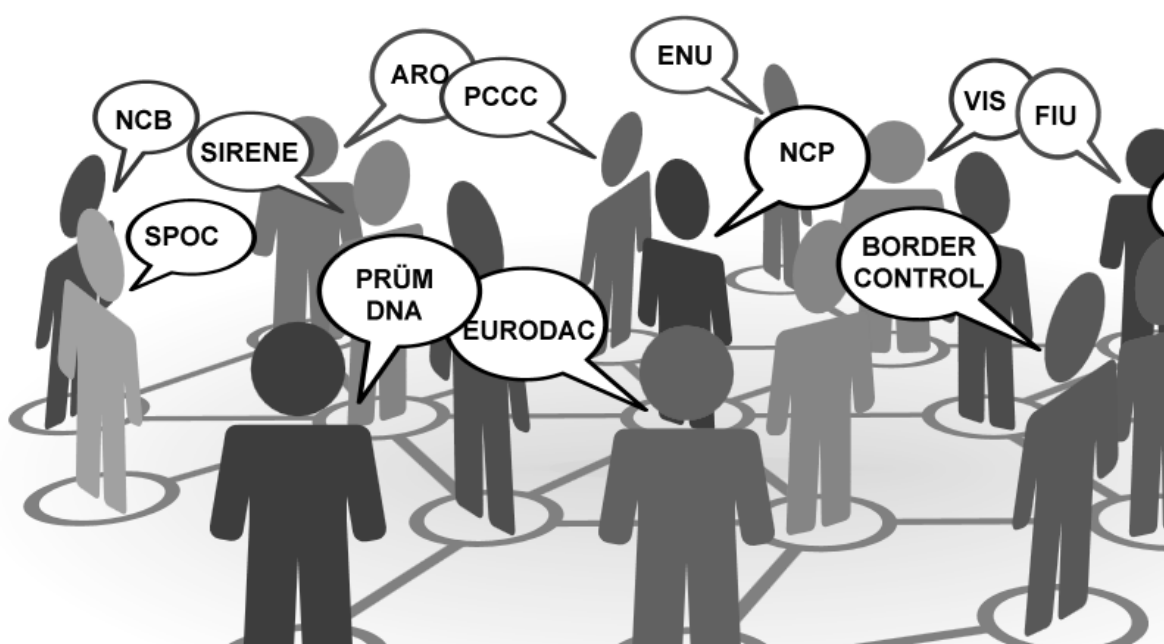
Elaborarea manualului propus a fost inclusă ca acțiune în cea de a 3-a listă de acțiuni a Strategiei de gestionare a informațiilor, iar prima versiune a manualului a fost elaborată în timpul președințiilor irlandeză, cipriotă, elenă, italiană și letonă.

În vederea facilitării în continuare a utilizării Manualului privind schimbul de informații în materie de aplicare a legii, Președinția transmite versiunea actuală și actualizată delegațiilor și le invită să o difuzeze în mod adecvat, în funcție de nevoile lor.



Council of the European Union
General Secretariat
Directorate-General Justice and Home Affairs
Directorate Home Affairs
Unit 1C Police and Customs cooperation

Manual for Law Enforcement Information Exchange



© queidea - Fotolia.com

Cuprins

Introducere	9
LISTA DE VERIFICARE A: SCHIMBUL DE INFORMAȚII ÎN SCOPUL PREVENIRII ȘI INVESTIGĂRII INFRAȚIUNILOR	13
LISTA DE VERIFICARE B: SCHIMBUL DE INFORMAȚII ÎN SCOPUL COMBATERII INFRAȚIUNILOR DE TERORISM.....	20
LISTA DE VERIFICARE C: SCHIMBUL DE INFORMAȚII ÎN SCOPUL MENȚINERII ORDINII PUBLICE ȘI A SECURITĂȚII.....	27
PARTEA a II-a - Informații generale	30
1..... CANALE DE CONTACT	31
1.1. SPOC - punctul unic de contact	31
1.2. Birourile SIRENE	35
1.3. Unitatea națională EUROPOL (ENU)	36
1.4. Birourile centrale naționale (BCN) INTERPOL.....	37
1.5. Punctele de contact naționale Prüm	38
1.5.1. Punctul de contact național (PCN) Prüm – ADN și amprente digitale.....	38
1.5.2. Punctul de contact național (PCN) Prüm - datele privind înmatricularea vehiculelor (VRD)	40
1.5.3. PCN Prüm pentru prevenirea terorismului.....	41
1.5.4. PCN Prüm pentru evenimente majore	41
1.6. Punctele naționale (polițienești) de informare fotbalistică (PNIF)	42
1.6.1. Manualul privind fotbalul	43
1.7. Centre de cooperare polițienească și vamală (CCPV)	44
1.8. Ofițerii de legătură	46

1.9.	Birouri de recuperare a activelor (ARO) din statele membre	48
1.10.	Spălarea de bani – cooperarea dintre unitățile de informații financiare (FIU)	49
1.11.	Convenția Napoli II.....	51
1.12.	Unitatea de informații despre pasageri (UIP)	52
1.13.	Alegerea canalului – criterii utilizate în mod curent.....	55
2.	SISTEME DE INFORMAȚII	57
2.1.	Sistemul de informații Schengen de a doua generație (SIS II)	57
2.2.	EIS – sistemul informațional Europol.....	59
2.3.	SIENA – Aplicația de rețea a Europolului pentru schimbul securizat de informații	61
2.4.	I-24/7 – sistemul global de comunicații polițienești al Interpol.....	62
2.4.1.	Interpol: portalul ADN.....	62
2.4.2.	Baza de date a Interpolului cu amprente digitale	62
2.4.3.	Baza de date a Interpolului cu documente de călătorie furate și pierdute.....	63
2.4.4.	Tabelul de referință privind armele de foc.....	63
2.5.	ECRIS	64
2.6.	Sistemul de informații privind vizele (VIS).....	65
2.7.	Eurodac	66
2.8.	SIV - Sistemul de informații al vămiror.....	69
2.9.	Documente false și autentice on-line - FADO	70
2.10.	Registrul public online al documentelor autentice de identitate și de călătorie - PRADO	71
2.11.	Prezentare succintă a sistemelor informatice utilizate pentru schimbul de informații la nivelul UE	72
3....	LEGISLAȚIE - CONTEXTUL JURIDIC, NORMELE ȘI ORIENTĂRILE REFERITOARE LA PRINCIPALELE METODE ȘI SISTEME DE COMUNICARE.....	77
3.0.	Directiva privind protecția datelor	77
3.1.	„Decizia-cadru suedeză” (DCS).....	80
	SOLICITARE DE INFORMAȚII ȘI DATE OPERATIVE	88
	În temeiul Deciziei-cadru 2006/960/JAI a Consiliului	88
	I - Informații administrative	88
	II - Urgența	88
	Se solicită un tratament de urgență	88

III - Scopul	89
IV - Tipul informației	89
V - Codurile de utilizare	90
3.2. Schengen – schimbul de date în cadrul SIS II și în afara SIS II	91
3.3. Europol.....	94
3.4. Interpol	96
3.5. Ofițerii de legătură	97
3.6. Schimbul de date în temeiul Deciziei Prüm.....	99
3.7. Sistemul de informații privind vizele (VIS).....	101
3.8. Eurodac	102
3.9. Napoli II	103
3.9.1. Sistemul de informații al vămilelor - SIV	104
3.10. Birourile naționale de recuperare a activelor (ARO) și CARIN	105
3.11. Unitățile de informații financiare (FIU).....	106
3.12. Acordul UE-SUA privind Programul de urmărire a finanțărilor în scopuri teroriste (TFTP)	107
3.13. Schimbul de informații cu privire la cazierele judiciare (ECRIS)	109
3.14. Păstrarea datelor referitoare la telecomunicații.....	110
3.15. Directiva privind PNR (registrul cu numele pasagerilor)	112
3.16. Informații prelabile privind pasagerii (API).....	115
3.17. Încălcările normelor de circulație care afectează siguranța rutieră.....	116

INTRODUCERE

Scopul prezentului manual

Cooperarea polițienească transfrontalieră în interiorul Uniunii Europene se bazează în mare măsură pe schimbul de informații. Prezentul manual are drept scop facilitarea cooperării zilnice în acest scop. Principalul public-țintă al manualului este constituit din SPOC național, punctul unic de contact responsabil pentru gestionarea fluxului de informații între diferitele unități, și punctele de contact desemnate atât la nivel național, cât și la nivel internațional.

Cooperarea în materie de aplicare a legii în Europa se caracterizează prin creșterea și accelerarea schimburilor de informații. Pe de o parte, cooperarea este susținută de evoluția constantă a tehnologiilor informației și comunicațiilor. Pe de altă parte, există o supraabundență de baze de date disponibile, atât la nivel național, cât și internațional.

Prezentul manual urmărește să răspundă necesității de a găsi contactul sau baza de date adecvată într-un anumit context operațional. Manualul prezintă legislația relevantă fără a pierde din vedere scopul său principal: facilitarea schimbului transfrontalier de informații.

Structura manualului

Manualul este alcătuit din trei părți:

PARTEA I - „Contextul operațional” - conține o serie de tabele sau „liste de verificare” care corelează informațiile cuprinse în *PARTEA a II-a* și în *PARTEA a III-a* cu temeiul juridic pertinent sau cu informații privind punctul de contact. Respectivetele liste de verificare sunt împărțite în trei domenii tematice principale:

- **prevenirea și combaterea criminalității (și a imigrației ilegale) - lista de verificare A**
- **combaterea infracțiunilor de terorism - lista de verificare B**
- **menținerea ordinii publice - lista de verificare C**

Scopul acestor liste de verificare este de a orienta cititorul de la punctul ales drept canal sau metodă adecvată de comunicare într-un anumit context operațional către sursa informațiilor de contact sau către eventuale acte legislative, norme și dispoziții administrative și manuale de bune practici corespunzătoare.

PARTEA a II-a - „Informații generale” - prezintă imaginea de ansamblu în materie de aplicare a legii în ceea ce privește diversele metode și canale de comunicare aflate la dispoziția forțelor de poliție ale UE. Această a doua parte este alcătuită, la rândul ei, din trei domenii care se referă la:

- *canalele de comunicare (de exemplu, organismele implicate în schimbul de informații în materie de aplicare a legii)*
- *sistemele de informații și bazele de date utilizate în schimbul transfrontalier de date*
- *legislație - contextul legislativ și normele și orientările referitoare la principalele metode și sisteme de comunicare*

PARTEA a III-a - „Fișe naționale” - în addendum la prezenta notă, conține fișele naționale cu informații detaliate privind punctele de contact relevante pentru toate aspectele schimbului transfrontalier de informații la care se face trimitere în întregul document. Statele membre au obligația de a notifica de îndată Secretariatului General al Consiliului eventualele modificări. Prin actualizarea periodică a fișelor naționale în addendumul la manual, statele membre vor respecta numeroasele obligații de notificare asumate în temeiul diverselor instrumente. Acest lucru ar trebui să faciliteze gestionarea și găsirea respectivelor informații în viitor.

PARTEA I - Contextul operațional

LISTA DE VERIFICARE A: SCHIMBUL DE INFORMATII ÎN SCOPUL PREVENIRII ȘI INVESTIGĂRII INFRACTIUNILOR

Sistem de informații	Punct național de acces	Temei juridic	Manual
Sistemul de informații Schengen/SIS II	SIRENE (Biroul pentru solicitarea de informații suplimentare la intrarea pe teritoriul național)	Acquis-ul Schengen, astfel cum este prevăzut la articolul 1 alineatul (2) din Decizia 1999/435/CE a Consiliului din 20 mai 1999 JO L 239/1, 22.9.2000 Decizia 2007/533/JAI a Consiliului, JO L 205/63, 7.8.2007 Regulamentul (CE) nr. 1986/2006 JO L 381/1, 28.12.2006 Regulamentul (CE) nr. 1987/2006 JO L 381/4, 28.12.2006	Versiune revizuită a Catalogului actualizat al recomandărilor în vederea aplicării corecte a acquis-ului Schengen și al celor mai bune practici, documentul 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Decizia de punere în aplicare (UE) 2015/219 a Comisiei din 29 ianuarie 2015 de înlocuire a anexei la Decizia de punere în aplicare 2013/115/UE privind Manualul SIRENE și alte măsuri de punere în aplicare a Sistemului de Informații Schengen de a doua generație (SIS II) [notificată cu numărul C(2015) 326]

Europol/ Sistemul informațional Europol - sistemul de index EIS Fișierele de lucru pentru analiză - AWF	Unitatea națională Europol (ENU)	Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului, JO L 135, 24.5.2016, p. 53- 114 (aplicabil începând cu 1 mai 2017).	
Interpol/I-24/7	BCN (Biroul central național)	Normele Interpol privind prelucrarea datelor [III/IRPD/GA/2011(2014)] Norme privind controlul informațiilor și accesul la dosarele Interpol [II.E/RCIA/GA/2004(2009)]	
Căutare automatizată ADN/Prüm în baze de date naționale desemnate	Punctul de contact național Prima etapă: căutarea automatizată	Articolele 3 și 4 din Decizia 2008/615/JAI, JO L 210/1, 6.8.2008	
	A doua etapă: transmiterea de date suplimentare cu caracter personal și de alte informații	Legislație națională Decizia-cadru 2006/960/JAI a Consiliului (DCS) JO L 386/89, 29.12.2006, Rectificare în JO L 75/26, 15.3.2007	

Căutare automatizată amprente digitale/Prüm în baza de date națională AFIS	Punctul de contact național Prima etapă: căutarea automatizată	Articolul 9 din Decizia 2008/615/JAI a Consiliului JO L 210/1, 6.8.2008	
	A doua etapă: transmiterea de date suplimentare cu caracter personal și de alte informații	Legislație națională Decizia-cadru 2006/960/JAI a Consiliului (DCS)	
Date privind înmatricularea vehiculelor (VRD)/ căutare automatizată Prüm în bazele de date VRD	Punctul de contact național pentru cererile primite	Articolul 12 din Decizia 2008/615/JAI a Consiliului, JO L 210/1, 6.8.2008,	
	pentru cererile trimise	ca mai sus	
Date din registrul cu numele pasagerilor (PNR) Termen de punere în aplicare: 25 mai 2018	Unitatea de informații despre pasageri (UIP)	Directiva (UE) a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave JO L 119/132, 4.5.2016	

Sistemul de informații privind vizele/VIS	Punctele naționale centrale de acces	Decizia 2004/512/CE a Consiliului JO L 213/5, 15.6.2004 Decizia 2008/633/JAI a Consiliului JO L 218/126, 13.8.2008 Lista autorităților competente al căror personal autorizat în mod corespunzător este abilitat să introducă, să modifice, să șteargă sau să consulte date din Sistemul de informații privind vizele (VIS) (2016/C 187/04), JO C 187/4, 26.5.2016.	
---	--------------------------------------	--	--

Eurodac	Autoritățile naționale competente	Regulamentul (UE) nr. 603/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid și privind cererile autorităților de aplicare a legii din statele membre și ale Europol de comparare a datelor Eurodac în scopul asigurării respectării aplicării legii și de modificare a Regulamentului (UE) nr. 1077/2011 de instituire a Agenției europene pentru gestionarea operațională a sistemelor informatice la scară largă, în spațiul de libertate, securitate și justiție (reformare) JO L 180/1, 29.6.2013 Regulamentul (UE) nr. 604/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid JO L 180/31, 29.6.2013	
---------	-----------------------------------	---	--

SIV - Sistemul de informații al vămilor	Punctele naționale de acces	Decizia 2009/917/JAI a Consiliului privind utilizarea tehnologiei informației în domeniul vamal JO L 323/20, 10.12.2009	
Sistemul european de informații cu privire la cazierele judiciare/ECRIS	Autoritatea națională centrală	Decizia 2009/316/JAI a Consiliului JO L 93/33, 7.4.2009	Manualul neobligatoriu pentru operatorii ECRIS disponibil în format electronic pe site-ul CIRCABC https://circabc.europa.eu
Rețeaua Camden Inter-agenții de Recuperare a Bunurilor (CARIN)	Biroul de recuperare a activelor (ARO)	Decizia 2007/845/JAI a Consiliului din 6 decembrie 2007 privind cooperarea dintre oficiile de recuperare a creanțelor din statele membre în domeniul urmăririi și identificării produselor provenite din săvârșirea de infracțiuni sau a altor bunuri având legătură cu infracțiunile JO L 332/103, 18.12.2007	Manual de bune practici în lupta împotriva infracțiunilor financiare: o colecție de bune exemple de sisteme bine dezvoltate în statele membre pentru lupta împotriva infracțiunilor financiare Documentul 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37

FIU.NET	Unitățile de informații financiare (FIU)	Decizia 2000/642/JAI a Consiliului din 17 octombrie 2000 privind acordurile de cooperare între unitățile de informații financiare ale statelor membre în ceea ce privește schimbul de informații JO L 271/4, 24.1.2000 Directiva (UE) 2015/849 a Parlamentului European și a Consiliului din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului și de abrogare a Directivei 2005/60/CE a Parlamentului European și a Consiliului și a Directivei 2006/70/CE a Comisiei JO L 141/73, 5.6.2015	Manual de bune practici în lupta împotriva infracțiunilor financiare: o colecție de bune exemple de sisteme bine dezvoltate în statele membre pentru lupta împotriva infracțiunilor financiare Documentul 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37
---------	--	---	--

LISTA DE VERIFICARE B: SCHIMBUL DE INFORMAȚII ÎN SCOPUL COMBATERII INFRACTIUNILOR DE TERORISM

Sistem de informații	Punct național de acces	Temei juridic	Manual
Sistemul de informații Schengen/SIS II	SIRENE (Biroul pentru solicitarea de informații suplimentare la intrarea pe teritoriul național)	Acquis-ul Schengen, astfel cum este prevăzut la articolul 1 alineatul (2) din Decizia 1999/435/CE a Consiliului din 20 mai 1999 JO L 239/1, 22.9.2000 Decizia 2007/533/JAI a Consiliului, JO L 205/63, 7.8.2007 Regulamentul (CE) nr. 1986/2006 JO L 381/1, 28.12.2006 Regulamentul (CE) nr. 1987/2006 JO L 381/4, 28.12.2006	Versiune revizuită a Catalogului actualizat al recomandărilor în vederea aplicării corecte a acquis-ului Schengen și al celor mai bune practici, documentul 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Decizia de punere în aplicare (UE) 2015/219 a Comisiei din 29 ianuarie 2015 de înlocuire a anexei la Decizia de punere în aplicare 2013/115/UE privind Manualul SIRENE și alte măsuri de punere în aplicare a Sistemului de Informații Schengen de a doua generație (SIS II) [notificată cu numărul C(2015) 326]

Europol/ Sistemul informațional Europol - sistemul de index EIS Fișierele de lucru pentru analiză - AWF	Unitatea națională Europol (ENU)	Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului, JO L 135, 24.5.2016, p. 53- 114 (aplicabil începând cu 1 mai 2017).	
Interpol/I-24/7	BCN (Biroul central național)	Normele Interpol privind prelucrarea datelor [III/IRPD/GA/2011(2014)] Norme privind controlul informațiilor și accesul la dosarele Interpol [II.E/RCIA/GA/2004(2009)]	
Căutare automatizată ADN/Prüm în baze de date naționale desemnate	Punctul de contact național Prima etapă: căutarea automatizată	Articolele 3 și 4 din Decizia 2008/615/JAI, JO L 210/1, 6.8.2008	
	A doua etapă: transmiterea de date suplimentare cu caracter personal și de alte informații	Legislație națională Decizia-cadru 2006/960/JAI a Consiliului (DCS) JO L 386/89, 29.12.2006, Rectificare în JO L 75/26, 15.3.2007	

Căutare automatizată amprente digitale/Prüm în baza de date națională AFIS	Punctul de contact național Prima etapă: căutarea automatizată	Articolul 9 din Decizia 2008/615/JAI a Consiliului JO L 210/1, 6.8.2008	
	A doua etapă: transmiterea de date suplimentare cu caracter personal și de alte informații	Legislație națională Decizia-cadru 2006/960/JAI a Consiliului (DCS)	
Date privind înmatricularea vehiculelor (VRD)/ căutare automatizată Prüm în bazele de date VRD	Punctul de contact național pentru cererile primite	Articolul 12 din Decizia 2008/615/JAI a Consiliului, JO L 210/1, 6.8.2008	
	pentru cererile trimise	ca mai sus	
Căutare automatizată ADN/Prüm în baze de date naționale desemnate	Punctul de contact național Prima etapă: căutarea automatizată	Articolele 3 și 4 din Decizia 2008/615/JAI, JO L 210/1, 6.8.2008	<i>Ghid de punere în aplicare - schimbul de date privind ADN</i> Documentul 7148/15 DAPIX 40 CRIMORG 25 ENFOPOL 61
Rețeaua Prüm pentru transmiterea datelor cu caracter personal și a informațiilor specifice pentru prevenirea infracțiunilor de terorism	Punctul național de contact Prüm pentru combaterea terorismului	Articolul 16 din Decizia 2008/615/JAI a Consiliului JO L 210/1, 6.8.2008	

Date din registrul cu numele pasagerilor (PNR) Termen de punere în aplicare: 25 mai 2018	Unitatea de informații despre pasageri (UIP)	Directiva (UE) a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave JO L 119/132, 4.5.2016	
Sistemul de informații privind vizele/VIS	Punctele naționale centrale de acces	Decizia 2004/512/CE a Consiliului JO L 213/5, 15.6.2004 Decizia 2008/633/JAI a Consiliului JO L 218/126, 13.8.2008 Lista autorităților competente al căror personal autorizat în mod corespunzător este abilitat să introducă, să modifice, să șteargă sau să consulte date din Sistemul de informații privind vizele (VIS) (2016/C 187/04), JO C 187/4, 26.5.2016.	

Eurodac	Autoritățile naționale competente	Regulamentul (UE) nr. 603/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid și privind cererile autorităților de aplicare a legii din statele membre și ale Europol de comparare a datelor Eurodac în scopul asigurării respectării aplicării legii și de modificare a Regulamentului (UE) nr. 1077/2011 de instituire a Agenției europene pentru gestionarea operațională a sistemelor informatice la scară largă, în spațiul de libertate, securitate și justiție (reformare) JO L 180/1, 29.6.2013 Regulamentul (UE) nr. 604/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid JO L 180/31, 29.6.2013	
---------	-----------------------------------	---	--

Sistemul european de informații cu privire la cazierele judiciare/ECRIS	Autoritatea națională centrală	Decizia 2009/316/JAI a Consiliului JO L 93/33, 7.4.2009	Manualul neobligatoriu pentru operatorii ECRIS disponibil în format electronic pe site-ul CIRCABC https://circabc.europa.eu
Rețeaua Camden Inter-agenții de Recuperare a Bunurilor (CARIN)	Biroul de recuperare a activelor (ARO)	Decizia 2007/845/JAI a Consiliului din 6 decembrie 2007 privind cooperarea dintre oficiile de recuperare a creanțelor din statele membre în domeniul urmăririi și identificării produselor provenite din săvârșirea de infracțiuni sau a altor bunuri având legătură cu infracțiunile JO L 332/103, 18.12.2007	

FIU.NET	Unitățile de informații financiare (FIU)	Decizia 2000/642/JAI a Consiliului din 17 octombrie 2000 privind acordurile de cooperare între unitățile de informații financiare ale statelor membre în ceea ce privește schimbul de informații JO L 271/4, 24.1.2000 Directiva (UE) 2015/849 a Parlamentului European și a Consiliului din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului și de abrogare a Directivei 2005/60/CE a Parlamentului European și a Consiliului și a Directivei 2006/70/CE a Comisiei JO L 141/73, 5.6.2015	
---------	--	---	--

LISTA DE VERIFICARE C: SCHIMBUL DE INFORMATII ÎN SCOPUL MENȚINERII ORDINII PUBLICE ȘI A SECURITĂȚII

Sistem de informații	Punct național de acces	Temei juridic	
Rețeaua punctelor de contact permanente privind ordinea publică	Punctele de contact naționale	Articolul 3 litera (b) din Acțiunea comună 97/339/JAI din 26 mai 1997 adoptată de Consiliu în temeiul articolului K.3 din Tratatul privind Uniunea Europeană referitoare la cooperarea în domeniul ordinii și siguranței publice JO L 147/1, 5.6.1997	
Rețeaua Prüm pentru transmiterea datelor cu caracter personal și fără caracter personal pentru prevenirea infracțiunilor și menținerea ordinii publice și a securității pentru evenimente majore care au o dimensiune transfrontalieră	Punctul de contact național Prüm /Evenimente majore	Articolul 15 din Decizia 2008/615/JAI a Consiliului JO L 210/1, 6.8.2008 Legislație națională	

Rețeaua punctelor naționale de informare fotbalistică	Punctele naționale de informare fotbalistică/ PNIF	Decizia 2002/348/JAI a Consiliului din 25 aprilie 2002 privind siguranța la meciurile de fotbal de anvergură internațională JO L 121/1, 8.5.2002 Decizia 2007/412/JAI a Consiliului din 12 iunie 2007 de modificare a Deciziei 2002/348/JAI privind siguranța la meciurile de fotbal de anvergură internațională JO L 155/76, 15.6.2007	Recomandarea (2007/C 314/07) Consiliului din 6 decembrie 2007 privind un manual pentru autoritățile polițienești și de securitate privind cooperarea cu ocazia evenimentelor majore care au o dimensiune internațională JO C 314/4, 22.12.2007 Rezoluția Consiliului din 3 iunie 2010 privind un manual actualizat de recomandări pentru cooperarea polițienească internațională și de măsuri pentru prevenirea și ținerea sub control a violenței și dezordinii legate de meciurile de fotbal de anvergură internațională care implică cel puțin un stat membru JO C 165/1, 24.6.2010
---	---	---	--

Rețeaua de protecție a personalităților	Punctele naționale de acces	Decizia 2009/796/JAI a Consiliului din 4 iunie 2009 de modificare a Deciziei 2002/956/JAI privind crearea unei rețele europene de protecție a personalităților JO L 283/62, 30.10.2009	Manualul rețelei europene de protecție a personalităților Documentul 10478/13 ENFOPOL 173
Centre de cooperare polițienească și vamală	CCPV	Acorduri bilaterale	

PARTEA A II-A - INFORMATII GENERALE

1. CANALE DE CONTACT ¹

1.1. SPOC - punctul unic de contact

Numeroase puncte de contact naționale

Statele membre, atât în calitate de stat solicitat, cât și în calitate de stat solicitant, fac față creșterii fluxului transfrontalier de informații prin sporirea eficienței structurilor și rețelelor operaționale, atât la nivel național, cât și la nivel european. Multe dintre instrumentele juridice ale UE privind cooperarea transfrontalieră în materie de aplicare a legii solicită instituirea unor autorități/organisme/birouri competente specifice sau a unor puncte de contact naționale (PCN). Poliția, autoritățile vamale sau alte autorități competente autorizate prin dreptul național trebuie să facă schimb de informații între ele prin intermediul acestor puncte de contact naționale (PCN) desemnate care, într-un anumit stat membru, se pot afla în departamente diferite ale forțelor de poliție sau chiar în ministere diferite. Pentru a oferi o imagine de ansamblu, în partea a III-a a prezentului document sunt incluse liste cu punctele de contact naționale specifice pentru schimbul de informații la nivelul UE în domeniul schimbului de date legat de aplicarea legii, respectivele liste fiind emise și actualizate periodic de către SGC.

Principiul disponibilității - DCS

Schimbul de informații în materie de aplicare a legii și de date operative cu relevanță transfrontalieră ar trebui să respecte condițiile care decurg din „principiul disponibilității” pus în aplicare prin „Decizia-cadru suedeză” (DCS). Aceasta înseamnă că:

- un reprezentant al autorităților de aplicare a legii dintr-un stat membru care are nevoie de informații pentru a-și îndeplini atribuțiile le poate obține de la un alt stat membru și
- autoritățile de aplicare a legii din statul membru care deține respectivele informații le vor pune la dispoziție în scopul declarat, ținând seama de necesitățile investigațiilor aflate în desfășurare în respectivul stat membru și
- odată ce informațiile polițienești sunt disponibile într-un stat membru, acestea se partajează la nivel transfrontalier în aceleași condiții care reglementează schimbul de informații la nivel național, cu alte cuvinte, normele aplicate într-un caz transfrontalier **nu sunt mai stricte** decât cele aplicate schimburilor de date la nivel național („principiul accesului echivalent”).

¹ Organismele naționale implicate în schimbul de informații în materie de aplicare a legii.

Punctul unic de contact (SPOC)

Combinăția de cerințe stricte din Decizia-cadru suedeză și existența diferitelor strategii naționale pentru gestionarea diverselor inițiative privind schimbul de informații impun o abordare mai simplă și mai uniformă la nivelul statelor membre pentru a se asigura că toate cererile de informații transmise între agențiile de aplicare a legii din UE sunt abordate în mod eficace și eficient.

Concluziile Consiliului privind modelul european de schimb de informații (EIXM)², adoptate în iunie 2013, au recunoscut potențialul unui punct unic de contact pentru schimbul de informații în interiorul fiecărui stat membru pentru a contribui la simplificarea procesului, într-un context juridic și operațional din ce în ce mai complex.

Politica de efectuare a cât mai multor schimburi de informații posibil prin intermediul unui punct unic de contact a fost pusă în aplicare de aproape toate statele membre, cu toate că înțelegerea a ceea ce definește un SPOC pare să varieze între statele membre. Orientările privind SPOC³ indică modul în care SPOC pot fi structurate pentru a utiliza la maximum resursele, pentru a evita suprapunerile și pentru a face cooperarea cu alte state membre mai eficientă, mai rapidă și mai transparentă.

Statele membre ar trebui să selecteze din aceste orientări soluția adecvată pentru situația lor, în vederea îndeplinirii obiectivului comun și convenit de consolidare a cooperării internaționale, și să examineze modalități adecvate de informare a altor state membre cu privire la soluția selectată, în vederea schimbului de bune practici.

² Concluziile Consiliului în urma Comunicării Comisiei privind modelul european de schimb de informații (EIXM), documentul 9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146.

³ „Proiect de orientări pentru un punct de contact unic destinat schimbului internațional de informații privind aplicarea legii”, documentele 10492/14 DAPIX 75 ENFOPOL 157 și 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1.

În mod ideal, punctul unic de contact:

- are acces la gama cea mai largă de baze de date naționale, europene și internaționale în materie de aplicare a legii, pentru a gestiona cu promptitudine schimburile directe de informații dintre autoritățile naționale competente;
- găzduiește unitățile naționale SIRENE, Europol și Interpol;
- găzduiește punctele de contact pentru ofițerii de legătură, punctele de contact desemnate în temeiul DCS și al „Deciziilor Prüm” și eventualele puncte de contact pentru birourile regionale și bilaterale;
- este instituit într-un mediu de lucru securizat și dispune de personal suficient și adecvat, inclusiv de capacități de interpretare sau traducere, pentru a funcționa 24/7. În măsura în care este posibil, toți membrii personalului ar trebui să fie instruiți și echipați/mandați să îndeplinească toate tipurile de atribuții în cadrul punctului unic de contact. În cazul în care acest lucru nu este posibil, ar trebui să se asigure posibilitatea ca toate sarcinile să fie îndeplinite prin intermediul unor ofițeri de gardă 24/7;
- este o organizație multi-agenție compusă din personal care provine din/apartine unor servicii diferite și/sau ministere, inclusiv poliția judiciară, poliția de frontieră, autoritățile vamale și judiciare.

Structura tipică a unui birou național SPOC (punct unic de contact)

Unitatea centrală de cooperare polițienească operațională, Platforma pentru schimbul de informații

*S.C.C.O.Pol este o structură **interministerială** alcătuită din 67 de polițiști, jandarmi și funcționari vamali. Magistrații Biroului de cooperare internațională în materie penală (BEPI) din cadrul Ministerului Justiției desfășoară, de asemenea, în aceeași incintă, un serviciu de bază pentru validarea cererilor franceze de emitere a mandatelor europene de arestare și pentru înregistrarea în fișierul național cu persoanele căutate a cererilor de arestare și a notificărilor roșii străine.*

*Pentru a se asigura **caracterul transversal** al celor trei canale de cooperare, în august 2004 a fost desemnat un punct central de contact (CCP) în cadrul S.C.C.O.Pol. Principala sa funcție este de a asista serviciile franceze de aplicare a legii la alegerea celui mai bun instrument de cooperare polițienească în funcție de natura și de complexitatea unei investigații în curs de desfășurare.*

Acesta verifică legalitatea cererii, realizează primele verificări încrucișate și o redirecționează către cel mai adecvat canal de cooperare având în vedere cererea investigatorilor. Numai cererile în legătură cu o alertă Schengen intră în sfera de competență exclusivă a SIRENE Franța.

*Ca urmare a punerii în comun cu succes a resurselor, S.C.C.O.Pol gestionează, **24 de ore din 24**, circa **350 000 de mesaje pe an**, pe o **platformă unică sigură**, cu personal limitat.*

Competența realizată prin mai multe canale a S.C.C.O.Pol îi permite să asigure reprezentarea Franței în cadrul grupurilor europene (SIS/VIS, SIS/SIRENE, șefii ENU) sau în cadrul grupurilor Interpol (reuniunea ofițerilor de contact Interpol, grupul privind notificările) și să contribuie cu un punct de vedere operațional relevant pentru unitatea DRI responsabilă în Franța de monitorizarea organismelor de guvernare ale Interpolului și Europolului.

1.2. Birourile SIRENE

Birourile SIRENE sunt esențiale pentru operațiile și schimbul de informații SIS. În fiecare stat membru sunt înființate birouri permanente SIRENE (Solicitare de informații suplimentare la intrarea pe teritoriul național), ca parte a acquis-ului Schengen⁴, drept autoritatea desemnată cu responsabilitatea centrală pentru secțiunea națională a Sistemului de informații Schengen (SIS II). Acestea sunt punctul de contact pentru birourile SIRENE ale altor părți contractante și legătura cu autoritățile și agențiile naționale. SIS II este un sistem de tip răspuns pozitiv/răspuns negativ bazat pe căutări. În regim 24/7, birourile fac schimb de informații în legătură cu alertele SIS II⁵, o alertă însemnând un set de date care le permite autorităților să identifice persoane sau obiecte în vederea luării unor măsuri adecvate.

„Informații suplimentare” sunt definite drept acele informații care nu sunt stocate în SIS II, dar care sunt în legătură cu alertele introduse în SIS II și care urmează a fi transmise în cadrul schimbului de informații, la nivel bilateral sau multilateral, prin intermediul unor formulare:

- (i) pentru a permite statelor membre să se consulte sau să se informeze reciproc în cazul în care introduc o alertă;
- (ii) în urma obținerii unui rezultat, pentru a permite luarea unei măsuri adecvate;
- (iii) în cazul în care măsura necesară nu poate fi luată;
- (iv) în cazul în care se ia în considerare calitatea datelor din SIS II;
- (v) în cazul în care se iau în considerare compatibilitatea alertelor și prioritatea acestora;
- (vi) în cazul în care se iau în considerare drepturile de acces.

⁴ A se vedea Convenția de punere în aplicare a Acordului Schengen, JO L 239, 22.9.2000.

⁵ A se vedea Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II), JO L 205/63, 7.8.2007.

Schimbul de informații trebuie să se facă în conformitate cu dispozițiile Manualului SIRENE⁶ și utilizând infrastructura de comunicare.⁷ SIS II⁸ a sporit funcționalitățile în comparație cu predecesorul său, cum ar fi posibilitatea de a introduce amprente digitale și fotografii, noi tipuri de obiecte (aeronave, bărci, containere, mijloace de plată furate), precum și posibilitatea ca inițiatorul alertei să facă legături între diferite alerte. SIS II conține copii ale mandatelor europene de arestare (MEA) atașate direct alertelor privind persoanele vizate.

Birourile SIRENE facilitează cooperarea polițienească și pot avea de asemenea un rol în schimburile de informații care se înscriu în afara domeniului de aplicare a SIS II în temeiul dispozițiilor reglementate anterior de articolele 39 și 46 din CAAS care au fost înlocuite de „**Decizia-cadru suedeză**”. În conformitate cu articolul 12 alineatul (1) din „Decizia-cadru suedeză”, dispozițiile articolului 39 alineatele (1), (2) și (3) și ale articolului 46 din Convenția de punere în aplicare a Acordului Schengen (CAAS), în măsura în care se referă la schimbul de informații sau date operative cu scopul de a desfășura investigații sau operațiuni de colectare a datelor operative în materie penală în condițiile prevăzute de decizia-cadru, se înlocuiesc cu dispozițiile deciziei-cadru.

1.3. Unitatea națională EUROPOL (ENU)

Fiecare stat membru are o Unitate națională Europol desemnată (ENU) care reprezintă organismul de legătură dintre Europol și autoritățile naționale competente. Ofițerii de legătură ai ENU detașați la Europol ar trebui să asigure o legătură în regim 24/7 între sediul central al Europolului de la Haga și unitățile naționale Europol din cele 28 de state membre. De asemenea, Europol găzduiește ofițeri de legătură din 10 țări și organizații din afara UE. Rețeaua este sprijinită de canale securizate de comunicare puse la dispoziție de Europol.

⁶ Decizia de punere în aplicare a Comisiei din 26 februarie 2013 privind Manualul SIRENE și alte măsuri de punere în aplicare a Sistemului de informații Schengen de a doua generație (SIS II) [notificată cu numărul C(2013) 1043], JO 71/1, 14.3.2013.

⁷ Din cauza închiderii rețelei de e-mail SISnet, birourile SIRENE pot utiliza în prezent serviciul de e-mail sTESTA. Alte schimburi de informații pot avea loc prin intermediul rețelei sTESTA, SIENA sau prin canalele de comunicare I-24/7.

⁸ Raport al Comisiei către Parlamentul European și Consiliu privind evaluarea Sistemului de informații Schengen de a doua generație (SIS II) în conformitate cu articolul 24 alineatul (5), articolul 43 alineatul (3) și articolul 50 alineatul (5) din Regulamentul (CE) nr. 1987/2006 și cu articolul 59 alineatul (3) și articolul 66 alineatul (5) din Decizia 2007/533/JAI; documentul 15810/16 SIRIS 175 COMIX 860

Europol⁹ sprijină autoritățile de aplicare a legii ale statelor membre în vederea prevenirii și combaterii criminalității organizate, a criminalității internaționale grave și a terorismului care implică două sau mai multe state membre. Pentru a colecta, stoca, prelucra și analiza date cu caracter personal și pentru a face schimb de informații și de date operative, Europol depinde de introducerea de date de statele membre. Regulamentul Europol stabilește diferitele sarcini în materie de informare și normele privind utilizarea datelor și schimbul de date cu părți terțe pe baza unui regim solid de protecție și de securitate a datelor.

1.4. Birourile centrale naționale (BCN) INTERPOL

Birourile centrale naționale (BCN) de la sediile centrale ale polițiilor naționale joacă un rol central în ceea ce privește prelucrarea datelor în cadrul Sistemului de informații Interpol oferit de țările lor. Acestea au dreptul de acces direct la sistem, ceea ce include:

- înregistrarea, actualizarea și ștergerea datelor direct în bazele de date polițienești ale organizației, precum și crearea de legături între date;
- consultarea directă a acestor baze de date;
- utilizarea notificărilor Interpol și a circularilor pentru transmiterea cererilor de cooperare și a alertelor internaționale.

Birourile centrale naționale pot căuta și verifica încrucișat datele, în mod rapid, cu un acces direct 24/7 la bazele de date care conțin informații privind persoanele suspectate de terorism, persoanele căutate, amprente digitale, profiluri ADN, documente de călătorie pierdute sau furate, autovehicule furate, opere de artă furate etc.

⁹ Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului, JO L 135, 24.5.2016, p. 53-114 (aplicabil începând cu 1 mai 2017).

În măsura posibilului, birourile centrale naționale ar trebui să permită autorităților de cercetare penală din țara proprie implicate în cooperarea polițienească internațională să aibă acces la Sistemul de informații Interpol. Birourile centrale naționale controlează nivelul de acces la serviciile Interpol pe care îl dețin alți utilizatori autorizați din țările lor și pot solicita să fie informate cu privire la interogările bazelor lor de date naționale făcute de alte țări.

1.5. Punctele de contact naționale Prüm

„Deciziile Prüm”¹⁰ au deschis o nouă dimensiune transfrontalieră de combatere a criminalității prin oferirea de acces online transfrontalier reciproc la bazele naționale de date ADN, la sistemele automate de identificare a amprentelor digitale (AFIS) și la bazele de date privind înmatricularea vehiculelor (VRD). Pentru a furniza date, se desemnează un punct de contact național (PCN) pentru fiecare tip de schimb de date în fiecare stat membru participant¹¹. Protecția datelor și dispozițiile adaptate privind securitatea datelor țin seama îndeosebi de natura specifică a accesului online la aceste baze de date. Furnizarea de date cu caracter personal necesită un nivel adecvat de protecție și de securitate a datelor, testat și aprobat de comun acord de statele membre înainte de a lansa schimbul de date.

1.5.1. Punctul de contact național (PCN) Prüm – ADN și amprente digitale

În cazul datelor ADN și al datelor privind amprente digitale, compararea automatizată a datelor biometrice de referință se bazează pe un sistem de tip „hit/no hit” (răspuns pozitiv/negativ). Datele de referință nu permit identificarea imediată a persoanei vizate. În cazul unui rezultat pozitiv, PCN al statului membru care efectuează căutarea poate, în consecință, să solicite date specifice cu caracter personal suplimentare. Furnizarea unor astfel de date suplimentare trebuie să fie solicitată prin intermediul unor proceduri de asistență reciprocă, inclusiv prin intermediul celor adoptate în temeiul „Deciziei-cadru suedeze”, și este reglementată de dreptul național al statului membru solicitat, inclusiv de normele privind asistența judiciară ale acestuia.

¹⁰ Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, JO L 210/1, 6.8.2008. Decizia 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, JO L 210/12, 6.8.2008.

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

1.5.1.1. Orientări privind bunele practici referitoare la căutarea de amprente digitale

Atunci când folosește instrumentul Prüm de căutare automatizată a amprentelor digitale, un stat membru solicitant ar trebui să urmeze recomandările stabilite în documentul intitulat *Bune practici pentru consultarea bazelor de date ale statelor membre* (14885/1/08 REV1). Acest document recunoaște capacitățile limitate de căutare ale **bazelor de date dactiloscopice** și recomandă promovarea la nivel operațional a următoarelor practici:

- decizia de a consulta sau nu bazele de date cu amprente digitale ale statelor membre și ordinea în care astfel de căutări sunt efectuate și repetate sunt decizii investigative luate de la caz la caz și nu ar trebui să fie prestabilite în mod sistematic.
- ar trebui, în principiu, să nu se efectueze căutări în bazele de date cu amprente digitale ale altor state membre decât după ce au fost efectuate căutări în baza (bazele) de date a (ale) statului membru solicitant.
- decizia de a efectua căutări într-una sau mai multe baze de date ale statelor membre ar trebui să țină seama în special de:
 - gravitatea cazului;
 - și/sau de direcțiile de investigare existente, în special de informațiile care indică un stat membru sau un grup de state membre;
 - și/sau de cerințele specifice ale investigației.
- Ar trebui să se efectueze căutări generale numai în cazul în care bunele practici de la punctele 1-3 au fost epuizate.

Exemple de schimburi automatizate de date în temeiul Deciziilor Prüm ale Consiliului

În 2011, în baza națională de date ADN a Cehiei a fost introdus material genetic în timpul investigării unui omor. Persoana suspectată în cadrul investigației fugise în străinătate. Materialul genetic a fost obținut de pe un capăt de țigară aflat într-o scrumieră în apartamentul în care a fost săvârșită infracțiunea. Prin efectuarea de căutări în baza de date ADN austriacă, s-a descoperit că aceleași profil fusese prelucrat în Austria. Alte date cu caracter personal au fost schimbate de SPOC ale ambelor țări prin intermediul cooperării polițienești. Ulterior, departamentul de justiție penală din Austria a fost contactat și i-a fost solicitat să predea suspectul în vederea efectuării urmăririi penale în Republica Cehă prin intermediul asistenței judiciare în materie penală.

În 2005, în baza națională de date ADN a Cehiei a fost introdus un profil ADN în timpul investigării unei tâlhării. În 2014 a fost identificată o persoană suspectată după efectuarea unei căutări în baza de date ADN austriacă. Părții austriece i s-a solicitat să furnizeze o fotografie recentă și alte date cu caracter personal prin intermediul SPOC.

1.5.2. Punctul de contact național (PCN) Prüm - datele privind înmatricularea vehiculelor (VRD)

În ceea ce privește VRD, căutările pot fi efectuate după un număr complet de șasiu într-unul sau în toate statele membre participante sau după un număr complet de înmatriculare într-un anumit stat membru. Informațiile vor fi schimbate de punctele de contact naționale desemnate atât pentru cererile primite, cât și pentru cele transmise. Statele membre își acordă reciproc acces online la VRD naționale pentru

- (a) datele privind proprietarii sau, după caz, utilizatorii și
- (b) datele privind vehiculele.

Statele membre folosesc o versiune a aplicației informatice Sistemul european de informare privind vehiculele și permisele de conducere (EUCARIS) concepută special pentru a servi scopurilor Prüm de efectuare a unor astfel de căutări. Căutările VRD se deosebesc de căutările ADN și de amprente digitale prin aceea că, în cazul unui rezultat pozitiv, acestea produc atât date cu caracter personal, cât și date de referință. Ca și în cazul altor căutări automatizate, este de la sine înțeles faptul că furnizarea de date cu caracter personal face obiectul nivelului adecvat de protecție a datelor aplicat de statele membre destinate.

1.5.3. PCN Prüm pentru prevenirea terorismului

La cerere sau din proprie inițiativă, punctele de contact naționale desemnate pot face schimb de informații privind persoanele suspectate de săvârșirea de infracțiuni de terorism. Datele cuprind numele de familie, prenumele, data și locul nașterii persoanei suspectate și o descriere a împrejurărilor care conduc la convingerea că persoana vizată va săvârși infracțiuni legate de activități de terorism.

Statul membru care transmite datele poate stabili, în conformitate cu dreptul național, condițiile privind utilizarea unor asemenea date și informații de către statul membru destinatar, stat care trebuie să respecte eventuale astfel de condiții.

1.5.4. PCN Prüm pentru evenimente majore

Statele membre care găzduiesc evenimente majore care au o dimensiune internațională trebuie să asigure securitatea evenimentului, atât din perspectiva ordinii publice, cât și din perspectiva combaterii terorismului. În funcție de natura evenimentului (politic, sportiv, social, cultural sau de altă natură), o perspectivă poate fi mai relevantă decât cealaltă. Cu toate acestea, ambele aspecte trebuie luate în considerare chiar dacă este posibil să fie tratate de autorități diferite. O atenție specială este acordată fenomenului infractorilor violenți care călătoresc (IVC), în special cu privire la meciurile de fotbal internaționale.

În vederea prevenirii infracțiunilor și a menținerii ordinii și securității publice în cazul unor evenimente majore și al unor întruniri de masă similare (de natură politică, sportivă, socială, culturală sau de altă natură), al dezastrelor și al accidentelor grave cu impact transfrontalier, punctele de contact naționale desemnate își transmit reciproc, la cerere sau din proprie inițiativă,

- date fără caracter personal sau
- date cu caracter personal, în cazul în care eventuale condamnări definitive sau alte împrejurări îndreptățesc convingerea că persoanele vizate vor săvârși infracțiuni cu ocazia evenimentelor sau reprezintă o amenințare la adresa ordinii și securității publice.

Datele cu caracter personal pot fi prelucrate numai în scopurile prevăzute anterior și pentru evenimentele concrete pentru care acestea au fost furnizate. Datele furnizate trebuie să fie șterse de îndată ce scopurile menționate au fost realizate, în orice caz, după cel mult un an. Informațiile sunt furnizate în conformitate cu dreptul național al statului membru care transmite datele.

1.5.4.1. Manual pentru cooperarea în ceea ce privește evenimentele majore care au o dimensiune internațională¹²

Prezentul manual conține orientări și sugestii pentru autoritățile de aplicare a legii însărcinate cu asigurarea securității publice cu ocazia evenimentelor majore, cum ar fi Jocurile Olimpice sau alte evenimente sportive majore, a evenimentelor sociale sau a reuniunilor politice la nivel înalt.

Manualul, care este modificat și adaptat în mod constant în conformitate cu evoluția bunelor practici, conține orientări privind gestionarea informațiilor și gestionarea evenimentelor, precum și privind evaluări legate de evenimente și evaluări strategice. Formularele-tip anexate privesc:

- cereri de ofițeri de legătură;
- analiza de risc privind potențialii manifestanți și alte grupuri;
- schimbul de informații cu privire la persoane sau grupuri care reprezintă o amenințare teroristă;
- o listă de documente de referință;
- un tabel conținând punctele de contact naționale permanente privind ordinea publică.

1.6. Punctele naționale (polițienești) de informare fotbalistică (PNIF)¹³

Pe lângă PCN Prüm pentru evenimentele majore și cu o atenție specială pentru meciurile de fotbal internaționale, în fiecare stat membru un punct național de informare fotbalistică (PNIF) este însărcinat cu schimbul de informații relevante și dezvoltarea cooperării polițienești transfrontaliere. Informațiile tactice, strategice și operaționale pot fi utilizate chiar de PNIF sau pot fi transmise către autoritățile pertinente sau serviciile de poliție.

Contactele dintre serviciile de poliție din diferitele țări implicate într-un eveniment sunt coordonate și, dacă este cazul, organizate de către PNIF. Site-ul internet al punctelor naționale de informare fotbalistică (PNIF) găzduit de CIV (www.nfip.eu) diseminează informații și consultanță referitoare la opțiunile juridice sau de altă natură disponibile în ceea ce privește aspectele de siguranță și securitate aplicabile meciurilor de fotbal.

¹² Recomandarea 2007/C 314/02 a Consiliului din 6 decembrie 2007 privind un manual pentru autoritățile polițienești și de securitate privind cooperarea cu ocazia evenimentelor majore care au o dimensiune internațională (JO C 314/4, 22.12.2007).

¹³ Decizia 2002/348/JAI a Consiliului din 25 aprilie 2002 privind siguranța la meciurile de fotbal de anvergură internațională, JO L 121/1, 8.5.2002.

PNIF coordonează prelucrarea informațiilor referitoare la suporterii care prezintă un risc ridicat în vederea pregătirii și luării de măsuri corespunzătoare pentru a menține legea și ordinea cu ocazia unui meci de fotbal. Astfel de informații includ, în special, informații referitoare la persoane care reprezintă sau ar putea reprezenta un pericol pentru lege și ordine, precum și pentru securitate. Informațiile ar trebui să fie transmise utilizând formularele¹⁴ care figurează în anexa la Manualul privind fotbalul.

1.6.1. Manualul privind fotbalul¹⁵

Manualul privind fotbalul este anexat la Rezoluția 2006/C 322/01 a Consiliului și oferă exemple privind modul în care poliția ar trebui să coopereze la nivel internațional pentru prevenirea și ținerea sub control a violenței și a dezordinii legate de meciurile de fotbal. Conținutul constă, în special, în recomandări privind:

- gestionarea informațiilor de către forțele de poliție;
- organizarea cooperării între forțele de poliție;
- o listă de verificare pentru politica mass-media și strategia de comunicare (poliție/autorități).

¹⁴ Decizia 2007/412/JAI a Consiliului din 12 iunie 2007 de modificare a Deciziei 2002/348/JAI privind siguranța la meciurile de fotbal de anvergură internațională, JO L 155/76, 15.6.2007.

¹⁵ Rezoluția Consiliului privind un manual actualizat de recomandări pentru cooperarea polițienească internațională și de măsuri pentru prevenirea și ținerea sub control a violenței și dezordinii legate de meciurile de fotbal de anvergură internațională care implică cel puțin un stat membru („Manualul UE privind fotbalul”) (2016/C 444/01), JO C 444, 29.11.2016, p. 1-36.

1.7. Centre de cooperare polițienească și vamală (CCPV)

CCPV-urile sunt instituite pe baza unor acorduri bilaterale sau multilaterale, în conformitate cu articolul 39 alineatul (4) din Convenția de punere în aplicare a acordului Schengen (CAAS). În acordurile respective părțile contractante definesc o bază de cooperare transfrontalieră, inclusiv atribuțiile, cadrul juridic și procedurile de instituire și funcționare a centrelor. CCPV-urile reunesc personal din țări învecinate și sunt strâns legate de organismele naționale responsabile cu cooperarea internațională (PCN, BCN Interpol, ENU, birourile SIRENE).

CCPV-urile oferă consiliere și sprijin neoperațional poliției operaționale naționale, serviciilor vamale și altor agenții din zona de frontieră în care sunt situate. Personalul CCPV are misiunea de a furniza rapid informațiile solicitate în conformitate cu Decizia 2006/960/JAI a Consiliului („Decizia-cadru suedeză”).

La sfârșitul lui 2016, 8 din cele 59 de CCPV-uri existente erau legate de SIEAN, aplicația de rețea a Europolului pentru schimbul securizat de informații. Schimburile de informații prin intermediul CCPV-urilor se referă în special la mica criminalitate și la cea de gravitate medie, la fluxurile de migrație ilegală și la problemele de ordine publică. Astfel de informații pot include identificarea șoferilor sau verificarea gradului de adecvare și a autenticității documentelor de identificare și de călătorie.

Părțile contractante pot decide de comun acord să transforme un CCPV într-un centru regional de coordonare operațională aflat în slujba tuturor agențiilor implicate, în special în cazul unor incidente regionale (catastrofe naturale) sau evenimente majore (Jocurile Olimpice, Campionatul Mondial de Fotbal etc.).

Dacă un CCPV primește informații care sunt de competența unității naționale centrale, informațiile respective trebuie transmise imediat SPOC/unității centrale. În cazul în care CCPV primește informații de interes evident pentru Europol, poate transmite aceste informații ENU situate în cadrul SPOC care le va înainta Europolului.

Exemplu de schimb de informații prin intermediul unui CCPV

EPICC („Euregio Police Information and Cooperation Centre” - Centrul Euregio de informare și cooperare polițienească) este denumirea scurtă a CCPV Heerlen.

Acesta a fost creat ad-hoc (niciun instrument juridic specific) în 2005 la inițiativa „NeBeDeAgPol”, o asociație a șefilor de poliție din euroregiunea Meuse-Rin, situată în zona de frontieră dintre Țările de Jos, Belgia și Germania – una dintre cele mai dens populate zone de frontieră din Uniunea Europeană.

În cadrul acestui CCPV lucrează împreună circa treizeci de polițiști belgieni, germani și neerlandezi, pe o singură platformă.

Acești agenți au acces la fața locului la cea mai mare parte a conținutului bazelor de date ale țărilor lor respective. Acest lucru le permite să furnizeze - într-un termen foarte scurt - răspunsuri exacte, complete și fiabile la cererile de informații din partea poliției privind BE, DE sau NL. Schimbul de informații dintre cele trei delegații ale EPICC se face prin intermediul aplicației „SIENA” a Europolului.

EPICC colectează și analizează informațiile de care dispune poliția în regiunea de frontieră pentru a identifica, descrie și urmări probleme de securitate la frontieră (fenomene sau moduri de operare noi, grupuri de infractori care acționează în zona de frontieră, evenimente sau persoane care necesită o atenție specială etc.).

Datorită competențelor sale speciale și compoziției sale mixte, CCPV Heerlen poate oferi un sprijin eficient în pregătirea și executarea operațiunilor, investigațiilor sau măsurilor de supraveghere transfrontaliere.

1.8. Ofițerii de legătură

În conformitate cu articolul 47 din Convenția de punere în aplicare a Acordului Schengen (CAAS), statele membre „pot încheia acorduri bilaterale privind detașarea, pentru o perioadă determinată sau nedeterminată, de ofițeri de legătură aparținând [unui stat membru] pe lângă autoritățile de poliție ale [altor state membre]”. Rolul ofițerilor de legătură este să stabilească și să mențină contacte directe în vederea promovării și accelerării cooperării în scopul combaterii criminalității, în special prin acordarea de asistență. Ofițerii de legătură nu sunt abilitați să execute eventuale măsuri polițienești în mod autonom. Aceștia garantează o cooperare rapidă și eficientă, bazată pe contacte personale și pe încredere reciprocă, prin:

- facilitarea și accelerarea colectării și a schimbului de informații;
- executarea cererilor de asistență polițienească și judiciară reciprocă în materie penală;
- organizarea și asigurarea operațiunilor transfrontaliere.

Ofițerii de legătură pot fi detașați în alte state membre, țări terțe sau agenții ale UE ori organizații internaționale. Compendiul¹⁶ privind ofițerii de legătură ai autorităților de aplicare a legii, actualizat anual de Secretariatul General al Consiliului, explică activitatea și sarcinile ofițerilor de legătură și conține liste de ofițeri de legătură, inclusiv date de contact.

Pe baza experiențelor anterioare și în curs de desfășurare din mai multe țări-gazdă și pentru a permite o mai bună punere în comun a activităților statelor membre în legătură cu țările terțe, atât în ceea ce privește activitatea ofițerilor de legătură, cât și cooperarea tehnică, au fost identificate unele bune practici care figurează în compendiu. Se propune ca ofițerii de legătură ai statelor membre și autoritățile lor competente să aplice aceste bune practici ori de câte ori este cazul.

¹⁶ „Actualizarea Compendiului privind ofițerii de legătură ai autorităților de aplicare a legii” (2014), documentul 11996/14 ENFOPOL 221 JAIEX 55 COMIX 384.

Exemple tipice de schimburi de informații între ofițerii de legătură

- *Ofițerii de legătură pot avea sarcina de a asigura un contact pentru a stabili o cooperare directă în cazuri specifice, cum ar fi infracțiunile legate de droguri.*
- *Ofițerii de legătură pot oferi informații specifice privind normele și legislația națională referitoare la cooperarea polițienească internațională sau la asistența judiciară în materie penală.*
- *În anumite cazuri, ofițerii de legătură păstrează liste actualizate de autorități responsabile din statul lor membru.*
- *De asemenea, în unele state membre, ofițerii de legătură au fost însărcinați cu gestionarea cererilor de cooperare în temeiul articolului 17 din Decizia Prüm (operațiuni comune). De exemplu, ofițerului de legătură danez la Europol i-a fost solicitat de Republica Cehă să înainteze o cerere Danemarcei în vederea desemnării a 4 polițiști danezi care să ofere asistență în ceea ce privește un caz care implica ambele state membre.*

1.9. Birouri de recuperare a activelor (ARO) din statele membre

Infrațiunile financiare acoperă o gamă largă de activități, cum ar fi contrafacerea, corupția și fraudă (de exemplu, fraudele cu cărți de credit, fraudele ipotecare, medicale sau cu titluri de valoare, darea sau luarea de mită ori deturnarea de fonduri, spălarea de bani, furtul de identitate și evaziunea fiscală). O cooperare sporită se obține printr-o mai strânsă colaborare transfrontalieră între birourile de recuperare a activelor (ARO), unitățile de informații financiare (FIU) și poliția și autoritățile vamale¹⁷.

În urma adoptării Deciziei 2007/845/JAI a Consiliului din 6 decembrie 2007 privind cooperarea dintre oficiile de recuperare a creanțelor din statele membre în domeniul urmăririi și identificării produselor provenite din săvârșirea de infracțiuni sau a altor bunuri având legătură cu infracțiunile¹⁸, toate statele membre au înființat și desemnat între timp birouri de recuperare a activelor (ARO). Aceste unități specializate au evoluat într-o rețea strânsă de specialiști care pot face schimb de informații în mod direct cu privire la aspecte legate de recuperarea activelor prin intermediul sistemului SIENA. Sub auspiciile Comisiei Europene și Europolului, rețeaua ARO facilitează cooperarea dintre birourile de recuperare a activelor din statele membre, precum și discuțiile strategice și schimbul de bune practici. Biroul Europol privind activele provenite din săvârșirea de infracțiuni (ECAB) acționează ca punct focal pentru recuperarea activelor în interiorul UE.

Dispozițiile prevăzute în Directiva 2014/42/UE a Parlamentului European și a Consiliului din 3 aprilie 2014 privind înghețarea și confiscarea instrumentelor și produselor infracțiunilor săvârșite în Uniunea Europeană¹⁹ vor spori suplimentar eficiența cooperării dintre birourile de recuperare a activelor în cadrul Uniunii Europene. Statelor membre li se solicită să transpună directiva până la data de 4 octombrie 2016.

¹⁷ Manual de bune practici în lupta împotriva infracțiunilor financiare: o colecție de bune exemple de sisteme bine dezvoltate în statele membre pentru lupta împotriva infracțiunilor financiare, documentul 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144.

¹⁸ Decizia 2007/845/JAI a Consiliului din 6 decembrie 2007 privind cooperarea dintre oficiile de recuperare a creanțelor din statele membre în domeniul urmăririi și identificării produselor provenite din săvârșirea de infracțiuni sau a altor bunuri având legătură cu infracțiunile, JO L 332/103, 18.12.2007.

¹⁹ Directiva 2014/42/UE a Parlamentului European și a Consiliului din 3 aprilie 2014 privind înghețarea și confiscarea instrumentelor și produselor infracțiunilor săvârșite în Uniunea Europeană, JO L 127/39, 29.4.2014.

Rețeaua Camden Inter-agenții de Recuperare a Bunurilor (CARIN), înființată în 2004 pentru a sprijini identificarea, înghețarea, sechestrarea și confiscarea de bunuri legate de infracțiuni, la nivel transfrontalier, sporește schimbul reciproc de informații privind diferitele abordări naționale a căror sferă de aplicare se întinde în afara UE.

Începând din 2015, Rețeaua CARIN cuprinde specialiști din 53 de jurisdicții și 9 organizații internaționale, care servesc drept puncte de contact în scopul schimbului transfrontalier rapid de informații, la cerere sau din proprie inițiativă. ARO naționale cooperează între ele sau cu alte autorități care facilitează urmărirea și identificarea produselor provenite din săvârșirea de infracțiuni. Deși toate statele membre au înființat un ARO, există diferențe majore între statele membre în ceea ce privește structura organizațională, resursele și activitățile.

Schimbul de informații se poate realiza în conformitate cu dispozițiile privind protecția datelor ale statelor membre destinate și face obiectul aceluiași norme privind protecția datelor ca și când informațiile ar fi fost colectate în statul membru destinat. Trebuie promovat schimbul de informații spontan, în conformitate cu această decizie, aplicarea procedurilor și a termenelor prevăzute în Decizia-cadru suedeză.

1.10. Spălarea de bani – cooperarea dintre unitățile de informații financiare (FIU)²⁰²¹

Informațiile pertinente cu privire la orice fapt care ar putea constitui un indiciu al spălării de bani sau al finanțării terorismului ar trebui raportate către unitățile naționale de informații financiare (FIU). FIU analizează informațiile primite de la caz la caz cu scopul de a stabili legături între tranzacțiile suspecte și activitatea infracțională subiacentă pentru a preveni și a combate spălarea de bani și finanțarea terorismului. FIU servește drept unitate națională centrală pentru primirea, analizarea și difuzarea rezultatelor analizelor sale către autoritățile competente. Fiind independentă și autonomă din punct de vedere operațional, FIU își îndeplinește funcțiile în mod liber, inclusiv decizia autonomă de a analiza, solicita și difuza informații specifice.

²⁰ Decizia 2000/642/JAI a Consiliului din 17 octombrie 2000 privind acordurile de cooperare între unitățile de informații financiare ale statelor membre în ceea ce privește schimbul de informații, JO L 271/4, 24.10.2000

²¹ Directiva (UE) 2015/849 a Parlamentului European și a Consiliului din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului și de abrogare a Directivei 2005/60/CE a Parlamentului European și a Consiliului și a Directivei 2006/70/CE a Comisiei, JO L 141/73, 5.6.2015

Unitățile de informații financiare servesc și drept puncte naționale de contact pentru schimbul transfrontalier de informații. La fel ca agențiile de recuperare a activelor, acestea variază considerabil între statele membre în ceea ce privește structura organizațională, funcțiile și resursele. Acestea se află fie în subordinea autorităților judiciare sau în structura organelor de poliție, fie sunt create ca un „hibrid”, combinând competențe polițienești și de urmărire penală. Această diversitate poate crea uneori obstacole în cooperarea internațională.

Totuși, având în vedere caracterul transnațional al spălării banilor și al finanțării terorismului, coordonarea și cooperarea între FIU sunt extrem de importante. Pentru a se îmbunătăți această coordonare și cooperare și pentru a se asigura că rapoartele privind tranzacțiile suspecte ajung la FIU din statul membru în care raportul ar fi cel mai util, sunt prevăzute norme detaliate în Directiva (UE) 2015/849. Pentru a oferi în mod rapid, constructiv și eficient cea mai variată gamă de activități de cooperare transfrontalieră, statele membre ar trebui în special să se asigure că unitățile lor de informații financiare fac schimb de informații în mod liber, spontan sau la cerere cu unitățile de informații financiare din țări terțe.

Îmbunătățirea schimbului de informații dintre FIU în cadrul Uniunii, utilizarea instalațiilor securizate, în special, rețeaua informatică descentralizată FIU.NET. Toate cele 28 de FIU sunt conectate la FIU.NET. Aceasta s-a dezvoltat în ultimii ani dintr-un instrument securizat elementar pentru schimbul structurat, bilateral de informații într-un instrument securizat multifuncțional pentru schimbul multilateral de informații, cu funcții de gestionare a cazurilor, precum și de standardizare semiautomată a proceselor. În cadrul FIU.NET, fiecare caracteristică nouă și fiecare proces automat sunt opționale, neexistând o obligație în acest sens. Unitățile individuale de informații financiare pot decide ce posibilități și caracteristici oferite de FIU.NET să utilizeze, utilizând numai caracteristicile pe care le agreează și excluzându-le pe cele de care nu au nevoie sau pe care nu doresc să le utilizeze.

1.11. Convenția Napoli II²²

Statele membre își oferă asistență reciprocă în temeiul Convenției Napoli II pentru a preveni și a depista încălcările dispozițiilor vamale naționale și pentru a urmări în justiție și a sancționa încălcările dispozițiilor vamale comunitare și naționale. În ceea ce privește investigațiile penale, convenția stabilește proceduri conform cărora administrațiile vamale pot acționa în comun și face schimb de informații, din proprie inițiativă sau la cerere, privind activitățile de trafic ilicit.

Cererile sunt transmise în scris, într-una dintre limbile oficiale ale statului membru al autorității solicitate sau într-o limbă considerată acceptabilă de autoritatea respectivă. Un formular stabilește standardul în ceea ce privește comunicarea de informații. Autoritățile implicate comunică toate informațiile care pot ajuta la prevenirea, detectarea și urmărirea penală a încălcărilor. Acestea fac schimb de date cu caracter personal, adică toate informațiile privind o persoană fizică identificată sau identificabilă.

Pentru a oferi asistența cerută, autoritatea solicitată sau autoritatea competentă căreia aceasta din urmă i se adresează procedează ca și când ar acționa pe cont propriu sau la cererea altei autorități din propriul stat membru.

Manualul pentru Convenția Napoli II cu privire la asistența reciprocă și cooperarea între administrațiile vamale este divizat în trei părți, care prevăd:

- dispozițiile generale în documentul 13615/05 ENFOCUSTOM 61 + COR 1 (CZ);
- fișele naționale, astfel cum au fost actualizate în 2016, în documentul 15429/16 JAI 1028 ENFOCUSTOM 238;
- anexele, inclusiv modelele de formulare pentru comunicarea informațiilor, în documentul 13615/05 ENFOCUSTOM 61 ADD 1.

²² Actul Consiliului din 18 decembrie 1997 de elaborare, în baza articolului K.3 din Tratatul privind Uniunea Europeană, a Convenției cu privire la asistența reciprocă și cooperarea între administrațiile vamale, JO C24/1, 23.1.1998.

1.12. Unitatea de informații despre pasageri (UIP)

În cadrul Directivei 2016/681²³, fiecare stat membru instituie sau desemnează o unitate de informații despre pasageri (UIP)²⁴. Aceste unități au competența de a prelucra datele din registrul cu numele pasagerilor (PNR) primite de la transportatorii aerieni²⁵ și, în plus, constituie principalul canal pentru schimbul de informații dintre statele membre și cu Europol. Două sau mai multe state membre pot institui sau desemna o singură autoritate drept UIP comună.

Prelucrarea datelor din PNR servește în principal la evaluarea pasagerilor aerieni în vederea identificării persoanelor pentru care este nevoie de o examinare suplimentară din partea autorităților naționale competente în materie de prevenire, depistare, investigare și urmărire penală a infracțiunilor de terorism și a infracțiunilor grave. Directiva se aplică zborurilor extra-UE și se poate aplica și zborurilor intra-UE în cazul în care un stat membru decide în acest sens.

Evaluarea datelor din PNR facilitează identificarea persoanelor care, înainte de o astfel de evaluare, nu erau suspectate de implicare în infracțiuni de terorism sau în infracțiuni grave. În conformitate cu politica UE privind protecția datelor, prelucrarea unor astfel de date ar trebui să fie deopotrivă pertinentă și necesară și ar trebui să fie proporțională cu obiectivele de securitate specifice urmărite de directivă.

²³ Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, JO L 119/132, 4.5.2016.

²⁴ Statele membre asigură intrarea în vigoare a actelor cu putere de lege și a actelor administrative necesare pentru a se conforma directivei până la 25 mai 2018.

²⁵ Directiva nu aduce atingere posibilității statelor membre de a prevedea, în dreptul intern, un sistem pentru colectarea și prelucrarea datelor din PNR de la operatorii economici care nu sunt transportatori aerieni, cum ar fi agențiile de voiaj și operatorii de turism care oferă servicii legate de călătorii – inclusiv rezervarea de zboruri – pentru care colectează și prelucrează date din PNR, sau de la alți transportatori decât cei menționați în directivă, cu condiția ca aceste dispoziții ale dreptului intern să respecte dreptul Uniunii.

UIP au următoarele responsabilități:

- la nivel național, colectarea datelor din PNR de la transportatorii aerieni, stocarea și prelucrarea datelor respective și transferul acestora sau al rezultatului prelucrării acestora către autoritățile naționale competente;
- la nivelul Uniunii, schimbul datelor din PNR și al rezultatului prelucrării acestora
 - a) între ele. Cu toate acestea, în cazuri de urgență și în anumite condiții, autoritățile naționale competente sus-menționate pot solicita direct UIP a unui alt stat membru să le furnizeze date din PNR care sunt păstrate în baza de date a acestuia și
 - b) cu Europolul, care are dreptul, în limitele competențelor sale și în vederea îndeplinirii sarcinilor sale, să solicite astfel de date unităților de informații despre pasageri.

UIP își îndeplinesc sarcinile exclusiv într-un loc sigur pe teritoriul unui stat membru. Datele din PNR furnizate UIP trebuie să fie stocate într-o bază de date pentru o perioadă de cinci ani după transferul lor către UIP a statului membru de sosire sau de plecare. Cu toate acestea, la șase luni de la transferul lor, toate datele PNR trebuie să fie depersonalizate prin mascarea elementelor de date care sunt prevăzute în directivă și care ar putea servi la identificarea directă a persoanei vizate. Rezultatul prelucrării este păstrat de UIP numai pentru perioada necesară pentru informarea autorităților naționale competente pertinente și pentru informarea UIP ale altor state membre cu privire la un rezultat pozitiv.

UIP prelucrează numai datele enumerate în anexa I la directivă, în următoarele scopuri:

- efectuarea unei evaluări a pasagerilor înainte de sosirea/plecarea programată a acestora în/din statul membru, în vederea identificării persoanelor pentru care este nevoie de o examinare suplimentară din partea autorităților naționale și, dacă este cazul, a Europolului;
- oferirea unui răspuns, de la caz la caz, la cererea autorităților competente privind furnizarea și prelucrarea de date din PNR pentru cazuri specifice și punerea rezultatelor unei astfel de prelucrări la dispoziția autorităților respective și, dacă este cazul, a Europolului;
- analizarea datelor din PNR în vederea actualizării sau a definirii de noi criterii aplicate în scopul identificării pasagerilor care pot fi implicați într-o infracțiune de terorism sau într-o infracțiune gravă.

Atunci când efectuează aceste evaluări, UIP poate fie să confrunte datele din PNR cu bazele de date relevante în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave, în conformitate cu normele Uniunii și cu normele internaționale și naționale aplicabile acestor baze de date, fie să prelucreze datele din PNR în funcție de criterii predefinite pertinente. Aceste criterii predeterminate trebuie să aibă o destinație precisă și să fie proporționale și specifice. Unităților de informații despre pasageri le revine sarcina de a stabili și revizui regulat aceste criterii în cooperare cu autoritățile competente pertinente. Criteriile respective nu se bazează pe date sensibile cu caracter personal, cum ar fi rasa sau originea etnică, opiniile politice, religia sau convingerile filozofice, apartenența la un sindicat, starea de sănătate, viața sexuală sau orientarea sexuală.

În ceea ce privește persoanele identificate, UIP transmite toate datele din PNR pertinente și necesare sau rezultatul prelucrării acestora către UIP corespunzătoare din celelalte state membre. Aceste UIP vor transmite informațiile primite autorităților lor competente.

Responsabilul cu protecția datelor numit de către UIP răspunde de monitorizarea prelucrării datelor din PNR. Persoana vizată are dreptul de a contacta responsabilul cu protecția datelor, ca punct unic de contact, cu privire la toate aspectele legate de prelucrarea datelor din PNR ale persoanei vizate.

Toate transferurile de date din PNR efectuate de către transportatorii aerieni către UIP trebuie să aibă loc prin mijloace electronice care asigură securitatea tehnică. În acest sens, atât protocoalele comune pe care transportatorii aerieni trebuie să le respecte atunci când transferă date, cât și formatele de date compatibile care asigură posibilitatea citirii datelor de către toate părțile implicate sunt definite la nivelul UE.²⁶

²⁶ Decizia de punere în aplicare (UE) 2017/759 a Comisiei din 28 aprilie 2017 privind protocoalele comune și formatele de date care trebuie să fie utilizate de transportatorii aerieni la transferul datelor PNR către unitățile de informații despre pasageri, JO L 113/48, 29.4.2017.

1.13. Alegerea canalului – criterii utilizate în mod curent

Într-un stat membru, punctul unic de contact²⁷ are un rol esențial în determinarea celui mai adecvat și mai relevant canal, prin colectarea tuturor cererilor (atât primite, cât și transmise) tratate de unitate. În interesul eficienței, autoritățile naționale acordă un important grad de autonomie investigatorilor în alegerea canalului considerat ca fiind cel mai adecvat pentru investigație.

Canalele de comunicare cel mai frecvent utilizate sunt următoarele:

- SIRENE, prin intermediul punctelor de contact ale fiecărui stat Schengen pentru SIS
- Europol, prin intermediul unităților naționale Europol/ofițerii de legătură Europol
- Interpol, prin intermediul birourilor centrale naționale de la sediile centrale ale polițiilor naționale
- ofițerii de legătură
- canalele de asistență reciprocă utilizate între autoritățile vamale (Napoli II)
- canalele bilaterale bazate pe acorduri de cooperare la nivel național, regional și local (CCPV)

²⁷ Orientările pentru un punct de contact unic, documentele 10492/14 DAPIX 75 ENFOPOL 157 și 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1.

Normele generale prevăd că o cerere se trimite printr-un singur canal. Cu toate acestea, în cazuri excepționale, o cerere poate fi trimisă prin canale diferite în același timp. În astfel de cazuri, acest lucru ar trebui să fie indicat în mod clar tuturor părților în mod corespunzător. În mod similar, o schimbare de canal trebuie comunicată tuturor părților, împreună cu motivul schimbării.

În vederea evitării suprapunerilor tematice sau a situațiilor în care o cerere este trimisă în mod inutil de mai multe ori prin diferite canale, funcționarul responsabil (SIS, Europol, Interpol, ofițerul de legătură bilateral) din statul solicitant poate determina cea mai adecvată cale pentru cererea de informații, pe baza următoarelor criterii:

- **criterii geografice**, de exemplu cetățenia/reședința/originea persoanei sau a obiectului în cauză este cunoscută, iar cererea privește comunicarea unor detalii (adresă, număr de telefon, amprente digitale, ADN, înregistrare etc.)
- **criterii tematice**, de exemplu criminalitatea organizată, criminalitatea gravă, terorismul; confidențialitatea/sensibilitatea; canalele utilizate pentru cererile conexe precedente
- **criterii tehnice**, de exemplu necesitatea unor canale IT securizate
- **criterii de urgență**, de exemplu un risc imediat la adresa integrității fizice a unei persoane, pierderea imediată de probe, cererea de operații sau supraveghere transfrontalieră urgentă

2. SISTEME DE INFORMAȚII

2.1. Sistemul de informații Schengen de a doua generație (SIS II)²⁸

În prezent, Sistemul de informații Schengen de a doua generație („SIS II”) este operațional în 26 de state membre ale UE, precum și în cele patru țări care nu fac parte din UE, dar sunt asociate cooperării Schengen: Norvegia, Islanda, Elveția și Liechtenstein. Acesta sprijină cooperarea operațională dintre autoritățile polițienești și autoritățile judiciare în materie penală. Având în vedere că SIS este un sistem de cooperare polițienească și de control la frontieră, polițiștii, polițiștii de frontieră și funcționarii vamali desemnați, precum și autoritățile judiciare și cele competente în materie de vize din întreg spațiul Schengen pot consulta SIS²⁹.

Datele din SIS II pot fi căutate (sub rezerva unor norme stricte de protecție a datelor) 24/7 prin intermediul punctelor de acces din birourile SIRENE, la punctele de control la frontiere, pe teritoriul național și în consulatele din străinătate. Baza de date înregistrează date atât privind **persoane**, cât și **obiecte**, și permite schimbul de date în scopul prevenirii criminalității și al combaterii imigrației neregulamentare. Prin intermediul căutărilor online SIS, funcționarul stabilește rapid, pe baza unei abordări „hit/no hit” (răspuns pozitiv/negativ), dacă persoana controlată este menționată în baza de date sau nu.

Datele sunt denumite alerte, o alertă fiind un set de date care permite autorităților să identifice persoane sau obiecte pentru a lua măsurile corespunzătoare:

Alerte privind **persoane**, vizând atât cetățenii UE, cât și cetățenii din afara UE. Acestea facilitează măsuri precum:

- arestarea în vederea predării fie în temeiul mandatului european de arestare, fie în temeiul unor acorduri încheiate între UE și țări terțe, sau în vederea extradării;
- căutarea persoanelor dispărute;
- citații pentru a apărea în fața unei instanțe judecătorești în contextul unei proceduri penale sau al executării unei pedepse privative de libertate;

²⁸ Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II), JO L 205/63, 7.8.2007.

²⁹ O listă a autorităților naționale competente care au drept de acces la alerte se publică anual în *Jurnalul Oficial al Uniunii Europene*.

- supravegherea discretă și controalele specifice, în vederea reprimării infracțiunilor, a prevenirii amenințărilor la adresa securității publice sau a prevenirii amenințărilor la adresa securității naționale;
- refuzarea intrării în spațiul Schengen pentru resortisanți sau străini ca urmare a unei decizii administrative sau judiciare sau pe motive legate de amenințări la adresa ordinii publice sau a siguranței și securității naționale ori pe motive legate de nerespectarea reglementărilor naționale privind intrarea și șederea străinilor.

Alertele SIS II privind **obiecte** sunt introduse pentru controale discrete sau controale specifice, în scopul sechestrării, utilizării drept probe în cadrul procedurilor penale sau al supravegherii.

Respectivele alerte se pot referi la:

- vehicule, ambarcațiuni, aeronave, containere
- arme de foc
- documente furate
- bancnote
- bunuri furate, cum ar fi obiecte de artă, ambarcațiuni, nave.

Personalul Europolului autorizat special are dreptul, în limitele mandatului propriu, să acceseze și să consulte direct datele introduse în SIS II și poate solicita informații suplimentare din partea statului membru vizat.

Membrii naționali ai Eurojustului și asistenții acestora au dreptul, în limitele mandatului lor, să acceseze și să consulte datele introduse în SIS II.

2.2. EIS – sistemul informațional Europol³⁰

Regulamentul Europol introduce un nou concept pentru prelucrarea datelor, care este denumit în mod obișnuit conceptul de gestionare integrată a datelor (IDMC). IDMC poate fi definit ca fiind posibilitatea de a utiliza informații legate de infracțiuni în scopuri profesionale multiple, astfel cum o indică proprietarul datelor, permițând gestionarea și prelucrarea acestora într-un mod integrat și neutru din punct de vedere tehnologic. În temeiul Deciziei Europol a Consiliului, prelucrarea datelor a fost structurată în jurul sistemelor. Regulamentul Europol nu mai conține trimiteri la sisteme, în schimb impune indicarea scopurilor prelucrării. Pentru a se facilita o tranziție fără probleme, utilizatorii pot continua să lucreze cu sistemele existente într-un mod care să respecte noul cadru juridic.

Sistemul informațional Europol (EIS), menționat în Decizia Europol, este un sistem centralizat găzduit de Europol, care le permite statelor membre și partenerilor de cooperare ai Europolului să stocheze, să partajeze și să verifice încrucișat datele referitoare la persoanele suspectate, la persoanele condamnate sau la „potențiali viitori infractori” implicați în infracțiuni care intră sub incidența mandatului Europolului (criminalitate gravă, criminalitate organizată sau terorism). EIS permite stocarea întregii serii de date și probe referitoare la respectivele infracțiuni/persoane, de exemplu, persoane cu pseudonime, societăți, numere de telefon, adrese de e-mail, vehicule, arme de foc, ADN, fotografii, amprente digitale, bombe etc. EIS, care servește în primă instanță drept sistem de sprijinire a verificării încrucișate, oferă un acces de tip răspuns pozitiv/răspuns negativ.

Regulamentul Europol prevede accesul deplin la datele transmise pentru analiză strategică-tematică, însă numai accesul de tip răspuns pozitiv/răspuns negativ pentru datele care sunt furnizate pentru analiză operațională.

³⁰ Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului, JO L 135, 24.5.2016, p. 53-114 (aplicabil începând cu 1 mai 2017).

EIS este, de facto, un sistem de referință care contribuie la identificarea existenței informațiilor căutate într-unul din statele membre ale UE, din partea partenerilor de cooperare sau a Europolului. Acesta este disponibil direct în toate statele membre și personalului autorizat în mod corespunzător. În prezent, pot fi distinse trei modalități de încărcare a datelor de către statele membre:

- (a) inserarea manuală a datelor în EIS sau prin intermediul SIENA;
- (b) transferul semiautomat prin desfășurarea unei încărcări pe loturi în EIS;
- (c) transferul automat al datelor, utilizând un sistem automatizat de încărcare a datelor.

Marea majoritate a datelor din sistemul informațional Europol (EIS) sunt înregistrate prin intermediul unor sisteme de încărcare automată a datelor. Abordarea în materie de colectare de date de către statele membre s-a schimbat, accentul în ceea ce privește transmiterea datelor depăsându-se către entitățile care pot fi verificate încrucișat, cum ar fi persoane, autovehicule, numere de telefon și arme de foc.

Țările terțe nu pot introduce direct și nici nu pot verifica încrucișat date în EIS, însă, în conformitate cu articolul 23 alineatul (5) din Regulamentul Europol, le pot transmite către Europol. Europol va trebui mai întâi să evalueze dacă datele intră sub incidența mandatului său și numai atunci va accepta datele și va efectua verificarea încrucișată a datelor.

EIS, care permite schimbul de informații extrem de sensibile, dispune de un sistem robust care asigură confidențialitatea și securitatea. Securitatea este asigurată, de exemplu, de coduri de utilizare specifice. Acestea indică ce poate fi făcut cu anumite informații și cine are acces la ele. Codurile de utilizare sunt concepute astfel încât să protejeze sursa informațiilor și să asigure faptul că prelucrarea informațiilor se face în conformitate cu dorințele proprietarului informațiilor și în conformitate cu dreptul național al statului membru. EIS este acreditat pentru prelucrarea datelor până la nivelul EU RESTRICTED inclusiv.

2.3. SIENA – Aplicația de rețea a Europolului pentru schimbul securizat de informații

SIENA este sistemul de comunicații securizate al Europolului, destinat utilizării de către statele membre, de către Europol și de către partenerii săi de cooperare pentru a face schimb de informații operaționale și strategice și de date operative referitoare la criminalitate, inclusiv de date operaționale referitoare la persoane. SIENA este un sistem de transmitere de mesaje care oferă diferite tipuri de mesaje destinate unor scopuri diverse, inclusiv schimbului de date în conformitate cu „Decizia-cadru suedeză”.

La proiectarea și funcționarea SIENA s-a pus un accent deosebit pe securitate, pe protecția datelor și pe confidențialitate. SIENA a fost acreditat pentru schimbul de informații de nivelul EU CONFIDENTIAL. Schimbul de date prin intermediul SIENA implică responsabilități clare în materie de prelucrare a datelor. Pentru fiecare mesaj SIENA trimis, trebuie indicate clasificarea (nivelul de confidențialitate), codurile de utilizare și fiabilitatea sursei și a informațiilor.

Limba setată automat pentru interfața de utilizare a SIENA este engleza, iar interfața este multilingvă, permițându-le operatorilor SIENA să lucreze în propria limbă națională (propriile limbi naționale). Pe lângă schimbul de mesaje, operatorii SIENA pot efectua căutări și crea rapoarte statistice cu privire la datele schimbate prin intermediul SIENA.

SIENA sprijină schimburile bilaterale de date dintre statele membre și le permite acestora să facă schimb de date care nu se încadrează în mandatul Europolului. Atunci când se adresează unuia dintre partenerii de cooperare ai Europolului în materie de schimb de date, statele membre primesc o notificare prin intermediul SIENA conform căreia respectivul schimb ar trebui să aibă loc numai dacă se referă la infracțiuni care se încadrează în mandatul Europolului.

Europolul va trata informațiile schimbate prin intermediul SIENA numai în scop de prelucrare a datelor operaționale dacă Europolul este inclus ca destinatar în schimbul de date. În vederea auditului, toate schimburile de date prin intermediul SIENA sunt puse la dispoziția responsabilului cu protecția datelor al Europolului și a organismelor naționale de supraveghere.

SIENA sprijină schimbul de date structurat bazat pe formatul universal pentru mesaje (UMF). În prezent, entitatea UMF PERSON poate fi creată/afișată în aplicația web SIENA însăși. Modelul de date UMF complet este deja compatibil cu serviciul web SIENA.

2.4. I-24/7 – sistemul global de comunicații polițienești al Interpol

Rețeaua globală I-24/7 pentru schimbul de informații polițienești face legătura între secretariatul general al Interpol cu sediul la Lyon, Franța, birourile centrale naționale din 190 de țări și birourile regionale.

Sistemul informațional Interpol permite comunicarea directă a mesajelor între birourile centrale naționale. Toate bazele de date ale Interpol (cu excepția bazei de date privind imaginile referitoare la exploatarea sexuală a copiilor) sunt accesibile în timp real prin I-24/7 - sistemul global de comunicații polițienești al Interpol. Sistemul I-24/7 permite, de asemenea, țărilor membre să aibă acces reciproc la bazele naționale de date, utilizând o conexiune *business-to-business* (B2B). Țările membre gestionează și mențin propriile date naționale în materie penală și controlează transmiterea de date și accesarea acestora de către alte țări, precum și distrugerea datelor în conformitate cu legile lor naționale. Țările au și opțiunea de a pune datele respective la dispoziția comunității internaționale de aplicare a legii prin intermediul sistemului I-24/7.

2.4.1. Interpol: portalul ADN

Baza de date ADN a Interpol include o bază de date ADN internațională, un formular pentru solicitarea de căutări internaționale pentru schimburile bilaterale și un mijloc pentru transferul electronic standardizat securizat. Nu sunt păstrate date nominale care să lege un profil ADN de o anumită persoană. Portalul ADN este compatibil cu schimbul automat de date Prüm.

Țările membre pot accesa baza de date și, la cerere, accesul poate fi extins și în afara birourilor centrale naționale ale țărilor membre, la centre și laboratoare criminalistice. Poliția din țările membre poate transmite un profil ADN de la infractori, de la locurile săvârșirii infracțiunilor, de la persoane dispărute și cadavre neidentificate.

2.4.2. Baza de date a Interpolului cu amprente digitale

Utilizatorii autorizați din țările membre pot vizualiza, transmite și verifica încrucișat informațiile înregistrate prin intermediul unui sistem automat de identificare a amprentelor digitale (AFIS). Informațiile înregistrate sunt păstrate și transmise în formatul definit de Institutul Național de Standarde și Tehnologie (NIST). Orientările privind transmiterea amprentelor digitale și Orientările privind transmiterea urmelor papilare colectate la locul infracțiunii oferă asistență țărilor membre în ceea ce privește îmbunătățirea calității și cantității de înregistrări privind amprente digitale transmise AFIS al Interpolului.

2.4.3. Baza de date a Interpolului cu documente de călătorie furate și pierdute

Baza de date a Interpol de documente de călătorie furate și pierdute cuprinde informații cu privire la peste 45 de milioane de documente de călătorie declarate pierdute sau furate de 166 de țări. Această bază de date permite birourilor centrale naționale ale Interpol și altor organisme autorizate de aplicare a legii (cum ar fi funcționarii din domeniul imigrației și al controlului la frontieră) să verifice valabilitatea unui document de călătorie suspect. În scopul prevenirii și combaterii criminalității grave și organizate, autoritățile competente în materie de aplicare a legii ale statelor membre fac schimb de informații privind pașapoartele cu Interpol³¹.

2.4.4. Tabelul de referință privind armele de foc

Tabelul de referință privind armele de foc al Interpol permite investigatorilor să identifice în mod adecvat o armă de foc utilizată la săvârșirea unei infracțiuni (marcă, model, calibru etc.). Acesta conține peste 250 000 de referințe privind armele de foc și 57 000 de imagini de înaltă calitate. Rețeaua de informații balistice a Interpol este o platformă pentru schimbul internațional la scară largă de date balistice și pentru compararea datelor balistice, conținând peste 150 000 de înregistrări.

Sistemul Interpol privind gestionarea înregistrărilor și a urmăririi armelor de foc ilicite (iARMS) este o aplicație informatică care facilitează schimbul de informații și cooperarea între agențiile de aplicare a legii privind infracțiunile care au legătură cu armele de foc.

³¹ Poziția comună 2005/69/JAI a Consiliului privind schimbul de anumite date cu Interpol, JO L 27/61, 29.1.2005.

2.5. ECRIS³²

Sistemul european de informații cu privire la cazierele judiciare (ECRIS)³³, sistem bazat pe tehnologia informației, furnizează mijloacele electronice pentru informațiile referitoare la condamnări care urmează a fi schimbate între statele membre în format standardizat. ECRIS este utilizat pentru a notifica statelor membre condamnări ale propriilor resortisanți și pentru a transmite cereri de informații referitoare la condamnări, pentru a fi utilizate în proceduri penale și în alte scopuri, cum ar fi în scopuri administrative sau de ocupare a forței de muncă. De asemenea, este posibil să se facă cereri privind resortisanții unor țări terțe, în cazul în care există motive să se creadă că statul membru solicitat deține informații cu privire la persoana respectivă.

Cererile adresate ECRIS trebuie să primească răspuns în termen de 10 zile lucrătoare, dacă cererea este făcută pentru a fi utilizată în cadrul unor proceduri penale sau în scopuri de ocupare a forței de muncă, și în termen de 20 de zile lucrătoare în cazul în care cererea a fost făcută de o persoană pentru propria informare.

ECRIS nu este conceput în vederea înființării vreunei baze de date centralizate a cazierelor judiciare și se bazează pe o arhitectură informatică descentralizată în care toate cazierele judiciare se stochează exclusiv în bazele de date gestionate de statele membre. Schimbul de date se face electronic între autoritățile centrale desemnate ale statelor membre.

Informațiile trebuie transmise de statele membre în conformitate cu normele convenite și formatele standardizate și trebuie să fie cât mai complete cu putință, pentru a permite statului membru care le primește să prelucreză informațiile în mod corect și să identifice persoana. Mesajele sunt trimise în limbile oficiale ale statelor membre vizate sau într-o altă limbă acceptată de ambele state membre.

Secretariatul General al Consiliului a publicat un Manual neobligatoriu pentru operatori, care stabilește procedurile privind schimbul de informații și coordonarea acțiunilor operatorilor pentru dezvoltarea și funcționarea ECRIS, manualul fiind disponibil în format electronic pe site-ul Consiliului și pe site-ul internet CIRCABC găzduit de Comisia Europeană <https://circabc.europa.eu>. Cererile de acces la manual trebuie să fie trimise Secretariatului Consiliului. Cererile de acces la grupul restrâns de interese „Sprijin tehnic și de afaceri ECRIS” trebuie trimise Comisiei Europene.

³² Decizia-cadru 2009/315/JAI a Consiliului din 26 februarie 2009 privind organizarea și conținutul schimbului de informații extrase din cazierele judiciare între statele membre, JO L 93/23, 7.4.2009.

³³ Decizia 2009/316/JAI a Consiliului de instituire a Sistemului european de informații cu privire la cazierele judiciare (ECRIS) în aplicarea articolului 11 din Decizia-cadru 2009/315/JAI, JO L 93/33, 7.4.2009.

2.6. Sistemul de informații privind vizele (VIS)³⁴

Sistemul de informații privind vizele (VIS) este în principal un sistem de control al imigrației.

Acesta este un instrument utilizat pentru a facilita cooperarea la nivelul controlului la frontiere prin verificarea electronică și schimbul de date privind vizele între statele membre de la frontierele externe ale UE. Ca atare, acesta îi vizează pe resortisanții străini.

Autoritățile desemnate ale statelor membre (de exemplu, oficiile consulare, punctele de control la frontieră, poliția și autoritățile din domeniul imigrației)³⁵ și Europolul³⁶, în cadrul atribuțiilor sale, sunt autorizate să consulte VIS³⁷ în scopul prevenirii, depistării și investigării:

- infracțiunilor de terorism, adică a infracțiunilor prevăzute de dreptul intern care corespund infracțiunilor prevăzute la articolele 1-4 din Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului sau sunt echivalente cu acestea și a
- infracțiunilor grave, adică a tipurilor de infracțiuni care corespund celor prevăzute la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI sau sunt echivalente cu acestea („mandatul european de arestare”).

În conformitate cu DCS, informațiile cuprinse în VIS pot fi furnizate Regatului Unit și Irlandei de către autoritățile competente ale statelor membre ale căror autorități desemnate au acces la VIS, iar informațiile deținute în registrele naționale ale vizelor din Regatul Unit și Irlanda pot fi transmise autorităților competente de aplicare a legii ale celorlalte state membre.

³⁴ Decizia Consiliului din 8 iunie 2004 de instituire a Sistemului de informații privind vizele (VIS) (2004/512/CE), JO L 213/5, 15.6.2004.

³⁵ Lista autorităților competente al căror personal autorizat în mod corespunzător este abilitat să introducă, să modifice, să șteargă sau să consulte date din Sistemul de informații privind vizele (VIS) (2016/C 187/04), JO C 187/4, 26.5.2016.

³⁶ Decizia 2008/633/JAI a Consiliului privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave, JO L 218/129, 13.8.2008; Decizia Consiliului de stabilire a datei de la care produce efecte Decizia 2008/633/JAI privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave (2013/392/UE), JO L 198/45, 23.7.2013.

³⁷ La 16 aprilie 2015, Curtea de Justiție a anulat Decizia 2013/392/UE a Consiliului de stabilire a datei de la care produce efecte Decizia 2008/633/JAI privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave. Cu toate acestea, Curtea a precizat că efectele Deciziei 2013/392 sunt menținute până la intrarea în vigoare a unui nou act destinat să o înlocuiască.

VIS se bazează pe o structură centralizată și pe o platformă comună cu SIS II. Datele VIS sunt prelucrate în două etape. În prima etapă, datele includ date alfanumerice și fotografii. În a doua etapă, sunt prelucrate și introduse în VIS date biometrice și documente scanate. VIS include date privind cererile de viză, fotografii, amprente digitale, deciziile aferente ale autorităților competente în materie de vize și legăturile între aplicațiile conexe. VIS utilizează un sistem de corelare a datelor biometrice pentru a asigura compararea fiabilă a datelor dactiloscopice în scopul:

- verificării, adică al unui control în urma căruia se stabilește dacă amprente digitale scanate la punctul de trecere a frontierei corespund celor asociate datelor biometrice anexate vizei sau
- identificării, adică al unei comparări a amprentelor digitale luate la postul de trecere a frontierei cu conținutul întregii baze de date.

Din punct de vedere tehnic, VIS cuprinde trei niveluri, și anume nivelul central, național și local, ultimul cuprinzând oficiile consulare, punctele de trecere a frontierei și autoritățile de poliție și din domeniul imigrației. VIS și SIS II folosesc aceeași platformă tehnică, astfel încât accesarea datelor de către operatorii ambelor sisteme va fi reciprocă; de exemplu, operatorii VIS pot avea acces la datele din SIS II și viceversa.

2.7. Eurodac³⁸³⁹

Sistemul european pentru compararea datelor dactiloscopice ale solicitanților de azil (Eurodac) asistă inițial la stabilirea statului membru responsabil de examinarea cererilor de azil prezentate într-unul dintre statele membre și ulterior la facilitarea aplicării Convenției de la Dublin. Accesul la Eurodac în scopul prevenirii, depistării și investigării infracțiunilor de terorism sau a altor infracțiuni grave se acordă numai în cazuri bine definite.

³⁸ Regulamentul (CE) nr. 2725/2000 al Consiliului din 11 decembrie 2000 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Convenției de la Dublin, JO L 316/1, 15.12.2000.

³⁹ Regulamentul (UE) nr. 603/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid și privind cererile autorităților de aplicare a legii din statele membre și ale Europol de comparare a datelor Eurodac în scopul asigurării respectării aplicării legii și de modificare a Regulamentului (UE) nr. 1077/2011 de instituire a Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (reformare).

Regulamentul Eurodac nr. 603/2013 stabilește norme privind transmiterea de date dactiloscopice către unitatea centrală, înregistrarea acestor date și a altor date relevante în baza de date centrală pertinentă, stocarea datelor, compararea lor cu alte date dactiloscopice, transmiterea rezultatelor acestei comparații și blocarea și ștergerea datelor înregistrate.

Arhitectura sistemului Eurodac constă (a) într-o bază de date dactiloscopice centrală informatizată („sistem central”) care cuprinde o unitate centrală și un plan și un sistem care asigură continuitatea activității și (b) o infrastructură de comunicații între sistemul central și statele membre, care furnizează o rețea virtuală criptată dedicată datelor Eurodac („infrastructură de comunicații”).

Fiecare stat membru are un singur punct de acces național.

eu-LISA, instituită prin Regulamentul (UE) nr. 1077/2011⁴⁰, este responsabilă de gestionarea operațională a Eurodac și asigură, în cooperare cu statele membre, faptul că, în orice moment, sunt utilizate pentru sistemul central cele mai bune și mai sigure tehnologii și tehnici disponibile, în urma efectuării unei analize cost-beneficiu.

Orice stat membru poate transmite amprente digitale către unitatea centrală, cu scopul de a controla dacă un străin în vârstă de cel puțin 14 ani care se află ilegal pe teritoriul său a depus deja o cerere de azil în alt stat membru. Unitatea centrală compară aceste amprente digitale cu datele dactiloscopice transmise de alte state membre și deja înregistrate în baza de date centrală. Unitatea informează statul membru care a transmis datele cu privire la existența unui răspuns pozitiv („hit”), adică rezultatul comparației dintre amprente digitale înregistrate și transmise. Acest stat membru verifică rezultatul și efectuează identificarea definitivă în cooperare cu statele membre vizate.

Statele membre trebuie să se asigure legalitatea, exactitatea și securitatea datelor Eurodac. Orice persoană sau stat membru care a suferit un prejudiciu ca urmare a nerespectării dispozițiilor Eurodac are dreptul să obțină despăgubiri de la statul membru responsabil de prejudiciul suferit.

⁴⁰ Regulamentul (UE) nr. 1077/2011 al Parlamentului European și al Consiliului din 25 octombrie 2011 de instituire a Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție, JO L 286/1, 1.11.2011.

Regulamentul (UE) nr. 603/2013 prevede accesarea datelor Eurodac de către autoritățile desemnate ale statelor membre și de către Europol în scopul aplicării legii. În conformitate cu regulamentul, autoritățile desemnate pot prezenta o cerere motivată, în format electronic, pentru compararea datelor dactiloscopice cu cele stocate în sistemul central, doar dacă compararea cu următoarele baze de date nu a condus la stabilirea identității persoanei vizate:

- bazele de date dactiloscopice naționale;
- sistemele automatizate de identificare a amprentelor digitale (AFIS) ale tuturor celorlalte state membre în temeiul Deciziei 2008/615/JAI („Decizia Prüm”), atunci când comparațiile sunt tehnic disponibile, dacă nu există motive rezonabile de a crede că compararea cu astfel de sisteme nu ar conduce la stabilirea identității persoanei vizate. Astfel de motive rezonabile se includ în cererea motivată, în format electronic, de comparare cu datele din Eurodac, transmisă de autoritatea desemnată autorității de control.
- Sistemul de informații privind vizele (VIS), dacă sunt îndeplinite condițiile pentru o astfel de comparare prevăzute în Decizia 2008/633/JAI.

Următoarele condiții cumulative trebuie, de asemenea, să fie îndeplinite:

- a) compararea este necesară în scopul prevenirii, depistării sau investigării infracțiunilor de terorism sau a altor infracțiuni grave, ceea ce înseamnă că există o preocupare prioritară legată de securitatea publică care determină proporționalitatea căutării în baza de date.
- b) compararea este necesară într-un caz specific (și anume nu se efectuează comparații sistematice).
- c) există motive întemeiate pentru a considera că o astfel de comparare va contribui în mod substanțial la prevenirea, depistarea sau investigarea oricăreia din infracțiunile în cauză. Aceste motive întemeiate există, în special, în cazul unei suspiciuni confirmate conform căreia suspectul, autorul sau victima unei infracțiuni de terorism sau a altei infracțiuni grave se încadrează într-o categorie aflată sub incidența Regulamentului (UE) nr. 603/2013.

2.8. SIV - Sistemul de informații al vămilor⁴¹

Sistemul de informații al vămilor completează Convenția Napoli II⁴². Sistemul vizează consolidarea administrației vamale a statelor membre prin schimbul rapid de informații în vederea prevenirii, investigării și urmăririi penale a încălcărilor grave ale dreptului național și comunitar. De asemenea, SIV creează o bază de date pentru identificarea dosarelor vamale (FIDE) pentru a sprijini investigațiile vamale.

SIV, gestionat de Comisie, este un sistem centralizat de informații accesibil prin intermediul terminalelor în fiecare stat membru și în incinta Comisiei, a Europolului și a Eurojustului. Datele SIV pot fi accesate de către autoritățile naționale vamale, fiscale, agricole, din domeniul sănătății publice și de autoritățile naționale polițienești, de Europol și Eurojust. Numai autoritățile desemnate de statele membre⁴³ și Comisia au acces direct la datele conținute în SIV. Pentru a consolida complementaritatea, Europolul și Eurojustul au acces limitat la citirea datelor din SIV și FIDE.

SIV cuprinde date cu caracter personal cu referire la mărfuri, mijloace de transport, întreprinderi, persoane, bunuri și mijloace bănești reținute, sub sechestru sau confiscate. Datele cu caracter personal nu pot fi copiate din SIV decât pe alte sisteme de prelucrare a datelor în vederea analizelor operaționale sau de gestionare a riscului, la care pot avea acces numai analiștii desemnați de statele membre.

FIDE permite autorităților naționale responsabile de efectuarea anchetelor vamale ca, în momentul în care deschid un dosar de anchetă, să identifice alte autorități care ar fi putut ancheta o anumită persoană sau întreprindere.

⁴¹ Decizia 2009/917/JAI a Consiliului din 30 noiembrie 2009 privind utilizarea tehnologiei informației în domeniul vamal, JO L 323/20, 10.12.2009.

⁴² Convenție redactată în baza articolului K.3 din Tratatul privind Uniunea Europeană, cu privire la asistența reciprocă și cooperarea între administrațiile vamale, JO C 24/2, 23.1.1998.

⁴³ Punerea în aplicare a articolului 7 alineatul (2) și a articolului 8 alineatul (3) din Decizia 2009/917/JAI a Consiliului din 30 noiembrie 2009 privind utilizarea tehnologiei informației în domeniul vamal – liste actualizate ale autorităților competente, documentul 13394/11 ENFOCUSTOM 85.

2.9. Documente false și autentice on-line - FADO⁴⁴

Un sistem computerizat de arhivare a imaginilor care cuprinde documente false și autentice și care se bazează pe tehnologia internetului permite un schimb de informații rapid și sigur între Secretariatul General al Consiliului Uniunii Europene și controlorii de documente din toate statele membre, precum și din Islanda, Norvegia și Elveția. Sistemul permite compararea pe ecran a documentului original cu un document fals sau falsificat. În principal, sistemul conține documente ale statelor membre, precum și documente ale țărilor terțe din care există fluxuri periodice de imigrație către țările membre. Baza de date instituită de FADO include următoarele date:

- imagini ale documentelor autentice;
- informații privind tehnicile de securitate (elementele de securitate);
- imagini ale unor documente false sau falsificate tipice;
- informații privind tehnicile de falsificare și
- statistici privind detectarea documentelor false și falsificate și ale fraudelor de identitate.

Sistemul utilizează linii speciale pentru transmisia datelor între Secretariatul General al Consiliului și unitățile centrale situate în statele membre. În cadrul fiecărui stat membru, sistemul este consultat prin intermediul unei conexiuni securizate la internet dintr-o unitate centrală. Un stat membru poate utiliza sistemul pe plan intern pe teritoriul său, ceea ce presupune conectarea mai multor terminale la diferitele sale puncte de control la frontieră sau la alte autorități competente. Cu toate acestea, nu există o legătură directă între un punct de lucru, altul decât o unitate centrală națională, și punctul central din cadrul Secretariatului General.

În prezent, FADO este disponibil în 22 de limbi oficiale ale Uniunii Europene. Documentele sunt introduse de experți în materie de documente în oricare dintre limbi, iar descrierile standardizate sunt traduse automat. Prin urmare, documentele sunt imediat disponibile în toate limbile recunoscute de sistem. Informațiile suplimentare sub formă de text liber conținute sunt traduse ulterior de specialiști lingviști din cadrul Secretariatului General al Consiliului.

⁴⁴ Acțiunea comună (98/700/JAI) din 3 decembrie 1998 adoptată de Consiliu în temeiul articolului K.3 din Tratatul privind Uniunea Europeană referitoare la crearea unui Sistem European de Arhivare a Imaginilor (FADO), JO L 333/4, 9.12.1998.

2.10. Registrul public online al documentelor autentice de identitate și de călătorie - PRADO

În timp ce accesul la FADO este restricționat la controlorii de documente și pentru uz guvernamental, Registrul public online al documentelor autentice de identitate și de călătorie al Consiliului Uniunii Europene (PRADO) conține un subset de informații FADO puse la dispoziția publicului larg. Site-ul internet⁴⁵ este publicat în limbile oficiale ale UE de către Secretariatul General al Consiliului Uniunii Europene din motive de transparență și oferă un serviciu important pentru un număr mare de utilizatori din Europa, în special pentru organizațiile neguvernamentale cu necesitatea sau obligația legală de a verifica identități.

Site-ul conține descrieri tehnice, inclusiv informații privind elementele de securitate ale documentelor autentice de identitate și de călătorie. Informațiile sunt selecționate și furnizate de experți în materie de documente din statele membre, Islanda, Norvegia și Elveția.

În PRADO, utilizatorii pot, de asemenea, găsi linkuri către site-uri cu informații privind numere de documente invalide furnizate de către unele state membre, precum și de țări terțe și alte informații utile referitoare la verificarea identității și a documentelor, precum și la fraudarea acestora.

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

2.11. Prezentare succintă a sistemelor informatice utilizate pentru schimbul de informații la nivelul UE

Sisteme și baze de date IT	Temei juridic	Scop	Persoane vizate	Partajarea datelor
Sistemul de informații Schengen de a doua generație — SIS II	Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II) JO L 205/63, 7.8.2007	• Securitatea internă • Controale la frontieră • Cooperarea judiciară • Investigarea infracțiunilor	• Cetățenii UE • Resortisanții țărilor terțe	• VIS • Europol • Eurojust • Interpol
	Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen din a doua generație (SIS II) JO L 381/4, 23.12.2006	• Refuzul intrării sau interdicția de ședere • Politici privind azilul, imigrarea și repatrierea	• Resortisanți ai unor țări terțe care nu se bucură de drepturi de liberă circulație echivalente celor ale cetățenilor Uniunii	
Europol EIS	Articolele 11-13 din Decizia 2009/371/JAI a Consiliului din 6 aprilie 2009 privind înființarea Oficiului European de Poliție (Europol) JO L 121/37, 15.5.2009	• Criminalitatea gravă • Imigrația • Securitatea internă • Combaterea terorismului	• Cetățenii UE • Resortisanții țărilor terțe	• SIS II
Interpol I-24/7	Constituția Interpol		• Cetățenii UE • Resortisanții țărilor terțe	• SIS II • Europol • VIS

Interpol Documente de călătorie pierdute/furate (LSTD)	Poziția comună 2005/69/JAI a Consiliului privind schimbul de anumite date cu Interpol JO L 27/61, 29.1.2005	• Criminalitatea organizată și internațională • Securitatea internă	• Cetățenii UE • Resortisanții țărilor terțe	
ECRIS	Decizia 2009/316/JAI a Consiliului de instituire a Sistemului european de informații cu privire la cazierile judiciare (ECRIS) în aplicarea articolului 11 din Decizia-cadru 2009/315/JAI JO L 93/33, 7.4.2009	Procedurile penale	• Cetățenii UE • Resortisanții țărilor terțe	

VIS	Decizia Consiliului din 8 iunie 2004 de instituire a Sistemului de informații privind vizele (VIS) (2004/512/CE), JO L 213/5, 15.6.2004 Decizia 2008/633/JAI a Consiliului privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave, JO L 218/129, 13.8.2008 Decizia Consiliului de stabilire a datei de la care produce efecte Decizia 2008/633/JAI privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave (2013/392/UE), JO L 198/45, 23.7.2013	• Criminalitatea gravă • Securitatea internă • Combaterea terorismului	• Resortisanții țărilor terțe	• SIS II • Europol • Interpol
------------	--	--	---	---

Eurodac	Regulamentul (UE) nr. 603/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid și privind cererile autorităților de aplicare a legii din statele membre și ale Europol de comparare a datelor Eurodac în scopul asigurării respectării aplicării legii și de modificare a Regulamentului (UE) nr. 1077/2011 de instituire a Agenției europene pentru gestionarea operațională a sistemelor informatice la scară largă, în spațiul de libertate, securitate și justiție (reformare) JO L 180/1, 29.6.2013 Regulamentul (UE) nr. 604/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid JO L 180/31, 29.6.2013	• Imigrația • Criminalitatea gravă • Securitatea internă • Combaterea terorismului	• Resortisanții țărilor terțe	Europol
----------------	---	---	---	---------

Registrul cu numele pasagerilor (PNR)	Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave JO L 119/132, 4.5.2016	• Criminalitatea gravă • Securitatea internă • Combaterea terorismului	• Cetățenii UE • Resortisanții țărilor terțe	Europol
Informații prealabile privind pasagerii (API)	Directiva 2004/82/CE a Consiliului din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii JO L 261/24, 6.8.2004	• Controlul la frontieră • Imigrația	Resortisanții țărilor terțe	
SIV -	Decizia 2009/917/JAI a Consiliului din 30 noiembrie 2009 privind utilizarea tehnologiei informației în domeniul vamal JO L 323/20, 10.12.2009	• Combaterea traficului ilicit	• Cetățenii europeni • Resortisanții țărilor terțe	Europol
FADO	Acțiunea comună (98/700/JAI) din 3 decembrie 1998 adoptată de Consiliu în temeiul articolului K.3 din Tratatul privind Uniunea Europeană referitoare la crearea unui Sistem European de Arhivare a Imaginilor (FADO) JO L 333/4, 9.12.1998	• Lupta împotriva documentelor false • Politica de imigrare • Cooperarea polițienească	• Cetățenii europeni • Resortisanții țărilor terțe	

3. **LEGISLAȚIE - CONTEXTUL JURIDIC, NORMELE ȘI ORIENTĂRILE REFERITOARE LA PRINCIPALELE METODE ȘI SISTEME DE COMUNICARE**

3.0. **Directiva privind protecția datelor**⁴⁶

Directiva (UE) 2016/680, care abrogă Decizia-cadru 2008/977/JAI a Consiliului⁴⁷, stabilește normele specifice referitoare la

- protecția persoanelor fizice, indiferent de cetățenia sau de locul de reședință al acestora, în ceea ce privește prelucrarea, prin mijloace automate sau în alt mod, a datelor cu caracter personal de către poliție sau de către alte autorități de aplicare a legii în limitele activităților lor și
- schimbul de date cu caracter personal în cadrul Uniunii de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor.

Scopul acesteia este de a asigura același nivel de protecție pentru persoanele fizice prin instituirea de drepturi garantate din punct de vedere juridic în întreaga Uniune și de a preîntâmpina practicile discrepante care împiedică schimbul de date cu caracter personal între autoritățile competente.

Statele membre trebuie să transpună directiva până la data de 6 mai 2018. Cu toate acestea, în cazul în care acest lucru necesită un efort disproporționat, statele membre pot prevedea, în mod excepțional, că vor pune în aplicare, până la 6 mai 2023, dispozițiile de monitorizare pertinente pentru operațiunile din cadrul sistemelor de prelucrare automată instituite înainte de 6 mai 2016.

⁴⁶ Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, JO L 119/89, 4.5.2016.

⁴⁷ Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, JO L 350/60, 30.12.2008. Decizia-cadru se abrogă cu efect de la 6 mai 2018.

Termenul „autorități competente” cuprinde autorități publice precum autoritățile judiciare, poliția sau alte autorități de aplicare a legii, precum și orice alt organism sau altă entitate însărcinată prin dreptul intern să exercite autoritatea publică și competențe publice în sensul acestei directive. Activitățile autorităților de aplicare a legii se concentrează în principal asupra prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor. Astfel de activități pot include, de asemenea, activitățile polițienești desfășurate cu ocazia manifestațiilor, a evenimentelor sportive majore și a revoltelor. De asemenea, activitățile menționate includ menținerea legii și ordinii ca atribuții ale acestor autorități atunci când aceasta se impune pentru asigurarea protecției împotriva amenințărilor la adresa securității publice și la adresa intereselor fundamentale ale societății și pentru prevenirea acestor amenințări, care pot conduce la o infracțiune.

Prelucrarea datelor cu caracter personal în scopuri care nu intră în domeniul de aplicare al activităților menționate mai sus – sarcină pe care statele membre le-o pot, de asemenea, încredința autorităților de aplicare a legii – și prelucrarea datelor cu caracter personal, în măsura în care aceasta se încadrează în domeniul de aplicare al dreptului Uniunii, sunt reglementate de Regulamentul (UE) 2016/679⁴⁸. În plus, Directiva (UE) 2016/680 nu se aplică prelucrării datelor cu caracter personal în ceea ce privește activitățile privind securitatea națională, activitățile agențiilor sau ale unităților specializate pe probleme de securitate națională sau prelucrării datelor cu caracter personal de către statele membre atunci când acestea desfășoară activități legate de politica externă și de securitate comună⁴⁹.

În sensul Directivei privind protecția datelor:

- **„date cu caracter personal”** înseamnă orice informație privind o persoană fizică („persoana vizată”) identificată sau identificabilă, direct sau indirect, în special prin referire la un nume, la un număr de identificare, la date de localizare, la un identificator online sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

Statele membre prevăd dispoziții potrivit cărora autoritățile competente care prelucrează date cu caracter personal, după caz și în măsura posibilului, vor face o distincție clară între datele cu caracter personal ale diferitelor categorii de persoane vizate, cum ar fi (a) persoanele suspectate, (b) persoanele condamnate, (c) victimele și (d) alte părți care au legătură cu infracțiunea, ca de exemplu martorii.

⁴⁸ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), JO L 119/1, 4.5.2016.

⁴⁹ Titlul V capitolul 2 din Tratatul privind Uniunea Europeană (TUE).

„**prelucrare**” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau a seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

Datele cu caracter personal trebuie să fie prelucrate în mod legal și echitabil și numai în scopuri specifice prevăzute de lege. Pentru a fi legală, o astfel de prelucrare ar trebui să fie necesară pentru îndeplinirea unei sarcini de către o autoritate competentă în scopurile aplicării legii menționate anterior. Principiul prelucrării echitabile a datelor din domeniul protecției datelor cu caracter personal este o noțiune distinctă de dreptul la un proces echitabil, astfel cum este definit la articolul 47 din Cartă și la articolul 6 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale. Datele cu caracter personal trebuie să fie adecvate și relevante pentru scopurile în care sunt prelucrate.

Prelucrarea datelor cu caracter personal deosebit de sensibile care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, afilierea sindicală, prelucrarea datelor genetice, prelucrarea datelor biometrice cu unicul scop al identificării unei persoane fizice sau prelucrarea datelor privind sănătatea sau a datelor privind viața sexuală și orientarea sexuală a unei persoane fizice este autorizată numai atunci când este strict necesară și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate și numai cu respectarea unor condiții bine definite și restrictive.

Instituirea unor autorități naționale de supraveghere capabile să își exercite atribuțiile în deplină independență reprezintă un element esențial al protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor. Autoritățile de supraveghere ar trebui să monitorizeze aplicarea dispozițiilor adoptate în temeiul directivei și să contribuie la aplicarea consecventă a acestora în întreaga Uniune. Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea autorităților naționale competente și a persoanelor împuternicite de către operator, inclusiv în ceea ce privește monitorizarea de către autoritățile de supraveghere și eventualele măsuri adoptate de acestea, necesită o atribuire clară a responsabilităților.

Circulația datelor cu caracter personal la nivel transfrontalier poate pune în pericol capacitatea persoanelor fizice de a se proteja din punct de vedere juridic împotriva utilizării sau a divulgării ilegale a acestor date. În același timp, autoritățile de supraveghere pot constata că se află în imposibilitatea de a da curs unor plângeri sau de a efectua investigații referitoare la activități desfășurate în afara frontierelor lor. Eforturile lor de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere și de caracterul eterogen al regimurilor juridice. Prin urmare, este necesar să se promoveze o cooperare mai strânsă între autoritățile de supraveghere a protecției datelor pentru a le ajuta să facă schimb de informații cu omologii lor străini.

3.1. „Decizia-cadru suedeză” (DCS)⁵⁰

Ca o dezvoltare a dispozițiilor acquis-ului Schengen, Decizia-cadru 2006/960/JAI a Consiliului („Decizia-cadru suedeză” - DCS) stabilește, în special, norme privind termenele și formularele-standard pentru schimbul transfrontalier de informații⁵¹, la cerere prealabilă sau în mod spontan, între autoritățile competente de aplicare a legii desemnate ale statelor membre în scopul:

- prevenirii, depistării și investigării infracțiunilor sau activităților infracționale care corespund celor prevăzute în mandatul european de arestare sau sunt echivalente cu acestea⁵² sau
- prevenirii unei amenințări grave și iminente la adresa securității publice.

Autoritățile desemnate sunt obligate să răspundă în termen de cel mult opt ore în cazurile urgente, în măsura în care informațiile sau datele operative solicitate sunt accesibile în mod direct autorităților de aplicare a legii. Este posibil să nu se furnizeze informațiile în cazul în care:

- se află în joc securitatea națională,
- investigațiile în curs riscă să fie puse în pericol,
- solicitarea se referă la o infracțiune care se pedepsește cu închisoarea până la un an în temeiul dreptului statului membru solicitat,
- autoritatea judiciară competentă refuză accesarea informațiilor.

⁵⁰ Decizia-cadru 2006/960/JAI a Consiliului din 18 decembrie 2006 privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene, JO L 386/89, 29.12.2006, și corectată prin rectificare, JO L 75/26, 15.3.2007.

⁵¹ A se vedea infra, figura 1.

⁵² Documentul 8216/2/08 REV2, Versiunea finală a manualului european privind modalitățile de emitere a unui mandat european de arestare. Articolul 2 din Decizia-cadru 2002/584/JAI a Consiliului privind mandatul european de arestare stabilește domeniul de aplicare al mandatului european de arestare.

Termenii „informații și/sau date operative” cuprind următoarele două categorii:

- orice tip de informații sau date operative deținute de către autoritățile de aplicare a legii;
- orice tip de informații sau date operative deținute de către autoritățile publice sau de către entitățile private și care sunt accesibile autorităților de aplicare a legii fără a se lua măsuri coercitive.

Conținutul acestor categorii depinde de legislația națională. Tipul de informații disponibile în fiecare stat membru este prezentat în fișele naționale anexate la prezentul manual.

Datele trebuie partajate cu Europolul în măsura în care informațiile sau datele operative schimbate se referă la o infracțiune sau la o activitate infracțională care intră sub incidența mandatului Europolului. Informațiile și datele operative vor fi prelucrate în conformitate cu codurile de utilizare relevante ale Europolului. SIENA (aplicația de rețea a Europolului pentru schimbul securizat de informații) sprijină schimbul de informații în conformitate cu „Decizia-cadru suedeză”.

Statele membre se asigură că condițiile pentru schimbul transfrontalier de informații nu sunt mai stricte decât cele care se aplică pentru un caz intern. Autoritățile competente de aplicare a legii nu sunt, în special, obligate să solicite acordul sau autorizarea judiciară prealabilă pentru schimbul transfrontalier de informații, în cazul în care informațiile solicitate sunt disponibile la nivel național fără un astfel de acord sau autorizare. În cazul în care autorizarea judiciară este, totuși, necesară, autoritatea judiciară, la emiterea deciziei sale, trebuie să aplice aceleași norme în cazurile transfrontaliere ca în cazurile strict interne. Informațiile care necesită o autorizare judiciară sunt indicate în fișele naționale.

Deoarece formularul-standard de solicitare de informații sau date operative a fost considerat prea greoi de către practicieni, a fost elaborat un formular neobligatoriu pentru solicitarea de informații și date operative⁵³. În situația în care utilizarea respectivului formular simplificat nu este fezabilă, se preferă utilizarea unui formular diferit sau a unui text liber, nestructurat.

Cu toate acestea, aceste solicitări trebuie în toate cazurile să respecte cerințele prevăzute la articolul 5 din Decizia-cadru suedeză și să conțină cel puțin următoarele elemente obligatorii:

- informații administrative, adică statul membru solicitant, autoritatea solicitantă, data, numărul/numerele de referință, statul membru/statele membre solicitat(e);
- dacă se solicită tratarea în regim de urgență și, dacă da, care sunt motivele pentru aceasta;
- descrierea informațiilor sau a datelor operative solicitate;

⁵³ A se vedea infra, figura 2.

identitatea/identitățile (în măsura în care este/sunt cunoscută/cunoscute) a/ale persoanei/persoanelor sau bunului/bunurilor care face/fac obiectul principal al cercetării penale sau al operațiunii de colectare a datelor operative în materie penală, care justifică solicitarea de informații sau date operative (de exemplu descrierea infracțiunii/infracțiunilor, a împrejurărilor săvârșirii acesteia/acestora etc.);

- scopul pentru care informațiile și datele operative sunt solicitate;
- legătura dintre scop și persoana care face obiectul acestor informații și date operative;
- motivele pentru care se consideră că informațiile sau datele operative se află pe teritoriul statului membru solicitat;
- orice restricții privind utilizarea informațiilor care figurează în solicitare („coduri de utilizare”).

Statul membru solicitant poate alege oricare din canalele existente pentru comunicarea internațională în materie de aplicare a legii (SIRENE, Europol, Interpol, puncte bilaterale de contact). Statul membru care răspunde solicitării utilizează în mod normal același canal care a fost utilizat pentru solicitare. În situația în care, cu toate acestea, statul membru solicitat răspunde, din motive legitime, prin alt canal, autoritatea solicitantă este informată în legătură cu această schimbare. Limba utilizată în solicitare și în furnizarea de informații este cea prevăzută pentru utilizarea canalului respectiv.

O imagine de ansamblu a **acordurilor bilaterale sau de alt tip menținute** este anexată la prezentul manual.

ANNEX A

INFORMATION EXCHANGE UNDER COUNCIL FRAMEWORK DECISION 2006/960/JHA FORM TO BE USED BY THE REQUESTED MEMBER STATE IN CASE OF TRANSMISSION/DELAY/REFUSAL OF INFORMATION

This form shall be used to transmit the requested information and/or intelligence, to inform the requesting authority of the impossibility of meeting the normal deadline, of the necessity of submitting the request to a judicial authority for an authorisation, or of the refusal to transmit the information.

This form may be used more than once during the procedure (e.g. if the request has first to be submitted to a judicial authority and it later transpires that the execution of the request has to be refused).

Requested authority (name, address, telephone, fax, e-mail, Member State)	
Details of the handling agent (optional):	
Reference number of this answer	
Date and reference number of previous answer	
Answering to the following requesting authority	
Date and time of the request	
Reference number of the request	

Normal time limit under Article 4 of Framework Decision 2006/960/JHA	
The offence falls under Article 2(2) of Framework Decision 2002/584/JHA and the requested information or intelligence is held in a database directly accessible by a law enforcement authority in the requested Member State	Urgency requested → ☐ 8 hours
	Urgency not requested → ☐ 1 week
Other cases	→ ☐ 14 days

Information transmitted under Framework Decision 2006/960/JHA: information and intelligence provided
1. Use of transmitted information or intelligence ☐ may be used solely for the purposes for which it has been supplied or for preventing an immediate and serious threat to public security; ☐ is authorised also for other purposes, subject to the following conditions (optional):
2. Reliability of the source ☐ Reliable ☐ Mostly reliable ☐ Not reliable ☐ Cannot be assessed
3. Accuracy of the information or intelligence ☐ Certain ☐ Established by the source ☐ Hearsay-confirmed ☐ Hearsay- not confirmed

4. The result of the criminal investigation or criminal intelligence operation within which the exchange of information has taken place has to be reported to the transmitting authority

- ☐ No
☐ Yes

5. In case of spontaneous exchange, reasons for believing that the information or intelligence could assist in the detection, prevention or investigation of offences referred to in Article 2(2) of Framework Decision 2002/584/JHA:

DELAY – It is not possible to respond within the applicable time limit under Article 4 of Framework Decision 2006/960/JHA

The information or intelligence cannot be provided within the given time-limit for the following reasons:

It is likely to be given within:

- ☐ 1 day ☐ 2 days ☐ 3 days
☐ weeks
☐ 1 month

- ☐ The authorisation of a judicial authority has been requested.
The procedure leading up to the granting/refusal of the authorisation is expected to last ... weeks

REFUSAL — The information or intelligence:

- ☐ could not be provided and requested at national level; or
☐ cannot be provided, for one or more of the following reasons:

A — Reason related to judicial control which prevents the transmission or requires the use of mutual legal assistance

- ☐ the competent judicial authority has not authorised the access and exchange of the information or intelligence
- ☐ the requested information or intelligence has previously been obtained by means of coercive measures and its provision is not permitted under the national law
- ☐ the information or intelligence is not held
- by law enforcement authorities; or
 - by public authorities or by private entities in a way which makes it available to law enforcement authorities without the taking of coercive measures

- ☐ **B —** The provision of the requested information or intelligence would harm essential national security interests or would jeopardise the success of a current investigation or a criminal intelligence operation or the safety of individuals or would clearly be disproportionate or irrelevant with regard to the purposes for which it has been requested.

If case A or B is used, provide, if deemed necessary, additional information or reasons for refusal (optional):

- ☐ **D —** The requested authority decides to refuse execution because the request pertains, under the law of the requested Member State, to the following offence (nature of the offence and its legal qualification to be specified) which is punishable by one year or less of imprisonment

- ☐ **E —** The requested information or intelligence is not available

- ☐ **F —** The requested information or intelligence has been obtained from another Member State or from a third country and is subject to the rule of speciality and that Member State or third country has not given its consent to the transmission of the information or intelligence.

ANNEX B

INFORMATION EXCHANGE UNDER COUNCIL FRAMEWORK DECISION 2006/960/JHA REQUEST FORM FOR
INFORMATION AND INTELLIGENCE TO BE USED BY THE REQUESTING MEMBER STATE

This form shall be used when requesting information and intelligence under Framework Decision 2006/960/JHA

I — Administrative information

Requesting authority (name, address, telephone, fax, e-mail, Member State):	
Details of the handling agent (optional):	
To the following Member State:	
Date and time of this request:	
Reference number of this request:	

Previous requests

☐ This is the first request on this case

☐ This request follows previous requests in the same case

Previous request(s)			Answer(s)	
	Date	Reference number (in the requesting Member State)	Date	Reference number (in the requested Member State)
1.				
2.				
3.				
4.				

If the request is sent to more than one authority in the requested Member State, please specify each of the channels used:

☐ ENU/Europol Liaison Officer ☐ For information
☐ For execution

☐ Interpol NCB ☐ For information
☐ For execution

☐ Sirene ☐ For information
☐ For execution

☐ Liaison Officer ☐ For information
☐ For execution

☐ Other (please specify): ☐ For information
☐ For execution

If the same request is sent to other Member States, please specify the other Member States and the channel used (optional)

--

II — Time limits

Reminder: time limits under Article 4 of Framework Decision 2006/960/JHA

A — The offence falls under Article 2(2) of Framework Decision 2002/584/JHA

and

the requested information or intelligence is held in a database directly accessible by a law enforcement authority

→ The request is urgent → Time limit: 8 hours with possibility to postpone

→ The request is not urgent → Time limit: 1 week

B — Other cases: time limit: 14 days

☐ Urgency IS requested
☐ Urgency is NOT requested
Grounds for urgency (e.g.: suspects are being held in custody, the case has to go to court before a specific date):
Information or intelligence requested

Type of crime(s) or criminal activity(ies) being investigated
Description of the circumstances in which the offence(s) was (were) committed, including the time, place and degree of participation in the offence(s) by the person who is the subject of the request for information or intelligence:

Nature of the offence(s)	
A — Application of Article 4(1) or 4(3) of the Framework Decision 2006/960/JHA	
☐ A.1. The offence is punishable by a maximum term of imprisonment of at least three years in the requesting Member State AND A.2. The offence is one (or more) of the following:	
☐ Participation in a criminal organisation ☐ Terrorism ☐ Trafficking in human beings ☐ Sexual exploitation of children and child pornography ☐ Illicit trafficking in narcotic drugs and psychotropic substances ☐ Illicit trafficking in weapons, munitions and explosives ☐ Corruption ☐ Fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests ☐ Organised or armed robbery ☐ Illicit trafficking in cultural goods, including antiques and works of art ☐ Swindling ☐ Racketeering and extortion ☐ Counterfeiting and piracy of products ☐ Forgery of administrative documents and trafficking therein ☐ Forgery of means of payment ☐ Illicit trafficking in hormonal substances and other growth promoters	☐ Laundering of the proceeds of crime ☐ Counterfeiting of currency, including the euro ☐ Computer-related crime ☐ Environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties ☐ Facilitation of unauthorised entry and residence ☐ Murder, grievous bodily injury ☐ Illicit trade in human organs and tissue ☐ Kidnapping, illegal restraint and hostage-taking ☐ Racism and xenophobia ☐ Illicit trafficking in nuclear or radioactive materials ☐ Trafficking in stolen vehicles ☐ Rape ☐ Arson ☐ Crimes within the jurisdiction of the International Criminal Court ☐ Unlawful seizure of aircraft/ships ☐ Sabotage
→ The offence therefore falls under Article 2(2) of Framework Decision 2002/584/JHA → Article 4(1) (urgent cases) and 4(3) (non urgent cases) of Framework Decision 2006/960/JHA are therefore applicable as regards time limits for responding to this request	
Or	
☐ B — The offence(s) is(are) not covered under A. In this case, description of the offence(s):	
Purpose for which the information or intelligence is requested	
Connection between the purpose for which the information or intelligence is requested and the person who is the subject of the information or intelligence	
Identity(ies) (as far as known) of the person(s) being the main subject(s) of the criminal investigation or criminal intelligence operation underlying the request for information or intelligence	
Reasons for believing that the information or intelligence is in the requested Member State	
Restrictions on the use of information contained in this request for purposes other than those for which it has been supplied or for preventing an immediate and serious threat to public security	
☐ use granted ☐ use granted, but do not mention the information provider ☐ do not use without authorisation of the information provider ☐ do not use	

Figura 2:

SOLICITARE DE INFORMAȚII ȘI DATE OPERATIVE

În temeiul Deciziei-cadru 2006/960/JAI a Consiliului

I - Informații administrative

Statul membru solicitant	
Autoritatea solicitantă (denumire, adresă, număr de telefon, număr de fax, e-mail):	
Coordonatele agentului responsabil (facultativ):	
Data și ora prezentei cereri:	
Numărul de referință al prezentei cereri:	
Numere de referință anterioare	

Statul membru/Statele membre solicitat/e:		
Canal:		
☐ Ofițer de legătură ENU/Europol	☐ Spre informare	☐ Spre execuție
☐ BCN Interpol	☐ Spre informare	☐ Spre execuție
☐ SIRENE	☐ Spre informare	☐ Spre execuție
☐ Ofițer de legătură	☐ Spre informare	☐ Spre execuție
☐ Altele (a se preciza):	☐ Spre informare	☐ Spre execuție

II - Urgența

Se solicită un tratament de urgență	☐ Da ☐ Nu
Motive pentru tratamentul de urgență (de exemplu: persoanele suspectate se află în stare de arest preventiv, cauza trebuie adusă în fața instanței înaintea unei date stabilite):	
Articolul 2 alineatul (2) Infracțiunea intră sub incidența articolului 2 alineatul (2) din Decizia-cadru 2002/584/JAI privind mandatul european de arestare	☐ Da ☐ Nu

III - Scopul

Tipul de infracțiune/infracțiuni sau de activitate infracțională/activități infracționale care fac obiectul investigării
Descrierea: - circumstanțelor comiterii infracțiunii/infracțiunilor (de exemplu: timpul, locul, gradul de participare la infracțiune/infracțiuni a persoanei care face obiectul cererii de informații sau date operative) - motivelor pentru care se consideră că informațiile sau datele operative se află pe teritoriul statului membru solicitat - legăturii dintre scopul pentru care se solicită informațiile sau datele operative și persoana care face obiectul acestor informații sau date operative
☐ cerere de utilizare a informațiilor, dacă este posibil, ca mijloace de probă în temeiul legislației naționale (<i>facultativ</i>)

IV - Tipul informației

Identitatea/identitățile (în măsura în care este/sunt cunoscută/cunoscute) a/ale persoanei/persoanelor sau obiectului/obiectelor		
Persoana	Obiectul/Obiectele	
Nume:	Numărul de serie al armei:	
Nume la naștere:	Numărul documentului:	
Prenume:	Alt număr sau altă denumire de identificare:	
Data nașterii	Numărul de înmatriculare al vehiculului:	
Locul nașterii	Numărul de serie al vehiculului (VIN):	
Sexul: ☐ bărbat ☐ femeie ☐ necunoscut	Tipul documentelor:	
Cetățenia:	Datele de contact ale societății comerciale (numărul de telefon, adresa de e-mail, adresa, pagina de web):	
Informații suplimentare:	Informații suplimentare:	
Informațiile sau datele operative solicitate		
Persoana	Vehicul	Altele
☐ verificarea identității	☐ completarea datelor de identificare	☐ identificarea societății comerciale
☐ verificarea în bazele de date	☐ identificarea proprietarului	☐ verificarea societății comerciale în bazele de date
☐ identificarea adresei/locului de ședere	☐ identificarea șoferului	☐ verificarea documentelor în bazele de date
	☐ verificarea în bazele de date	☐ identificarea numărului de telefon/fax
		☐ identificarea deținătorului adresei de e-mail
Alte:		

V - Codurile de utilizare

Utilizarea informațiilor cuprinse în prezenta cerere este restricționată la scopurile pentru care acestea au fost comunicate sau pentru a preveni un pericol imediat și grav pentru siguranța publică

☐ pentru utilizarea exclusivă în cadrul activităților de poliție, nu al procedurilor judiciare

3.2. Schengen – schimbul de date în cadrul SIS II și în afara SIS II

Acordul Schengen, semnat la 14 iunie 1985, a fost completat prin Convenția de punere în aplicare a Acordului Schengen (CAAS)⁵⁴ în 1990, care a creat spațiul Schengen prin eliminarea controalelor de frontieră între statele Schengen, norme comune privind vizele și cooperare polițienească și judiciară. CAAS prevede o cerință generală privind cooperarea polițienească și dă dreptul autorităților polițienești să facă schimb de informații, în limitele sistemului lor juridic național respectiv.

Odată cu intrarea în vigoare a Tratatului de la Amsterdam în 1999, măsurile de cooperare prevăzute până atunci în cadrul Schengen au fost integrate în cadrul juridic al Uniunii Europene, aspectele legate de Schengen fiind în prezent soluționate de către organismele legislative ale UE. Protocolul Schengen anexat la Tratatul de la Amsterdam a stabilit modalitățile detaliate pentru acest proces de integrare.

Sistemul de informații Schengen (SIS) a fost înființat în temeiul dispozițiilor din Titlul IV al Convenției din 19 iunie 1990. Acesta constituie un instrument esențial pentru aplicarea acquis-ului Schengen. Acesta constituie de asemenea o măsură care urmărește să compenseze absența unor controale la frontierele interne asupra persoanelor în spațiul Schengen prin intermediul unui instrument pentru schimbul de informații între autoritățile competente.

Faptul că cadrul juridic care reglementează SIS constă în prezent în două instrumente separate, și anume un regulament în privința aplicării SIS la frontiere și o decizie a Consiliului în privința cooperării polițienești, nu aduce atingere faptului că SIS constituie un sistem de informații unic.

⁵⁴ Convenția de punere în aplicare a Acordului Schengen din 14 iunie 1985 dintre guvernele statelor din Uniunea Economică Benelux, Republicii Federale Germania și Republicii Franceze privind eliminarea treptată a controalelor la frontierele comune, JO L 239/19, 22.9.2000

Legislație

Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen din a doua generație (SIS II), JO L 381/4, 28.12.2006

Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II), JO L 205/63, 7.8.2007.

Dispoziții-cheie

Sistemul de informații Schengen (SIS) este atât un sistem de cooperare polițienească, cât și un sistem de control la frontieră și sprijină cooperarea operațională dintre autoritățile polițienești și autoritățile judiciare în materie penală. Polițiștii, polițiștii de frontieră și funcționarii vamali desemnați, precum și autoritățile judiciare și cele competente în materie de vize din întreg spațiul Schengen pot consulta SIS⁵⁵.

Sistemul de informații Schengen de a doua generație („SIS II”) este în prezent operațional în 26 de state membre ale UE, precum și în cele patru țări care nu fac parte din UE, dar sunt asociate cooperării Schengen: Norvegia, Islanda, Elveția și Liechtenstein.

- În privința cooperării polițienești, atât Regatul Unit, cât și Irlanda au solicitat să fie autorizate să participe, însă numai Regatul Unit a fost autorizat, în 2015, să încarce date în timp real din partea respectivă din SIS⁵⁶ cu titlu provizoriu ca primă etapă, permițând realizarea unei evaluări înaintea unei decizii finale de „punere în aplicare”. Regatul Unit și Irlanda nu participă la aplicarea SIS în scopul controlului la frontiere.

⁵⁵ O listă consolidată a autorităților naționale competente, care specifică pentru fiecare autoritate ce date poate căuta și în ce scop, se publică anual în Jurnalul Oficial al UE în temeiul articolului 31 alineatul (8) din Regulamentul SIS și al articolului 46 alineatul (8) din Decizia SIS II.

⁵⁶ Decizia de punere în aplicare (UE) 2015/215 a Consiliului din 10 februarie 2015 privind punerea în aplicare a dispozițiilor acquis-ului Schengen privind protecția datelor și privind punerea în aplicare cu titlu provizoriu a unor părți ale dispozițiilor acquis-ului Schengen referitoare la Sistemul de informații Schengen în ceea ce privește Regatul Unit al Marii Britanii și Irlandei de Nord, JO L 36/8, 12.2.2015

- Bulgaria, România⁵⁷ și Croația⁵⁸ aplică dispozițiile acquis-ului Schengen referitoare la cooperarea polițienească și controlul la frontiere. Acestora li s-a acordat accesul în timp real la SIS în scopul evaluării aplicării corecte a dispozițiilor acquis-ului Schengen referitoare la SIS. Odată ce aceste evaluări vor fi realizate în mod satisfăcător, o decizie separată a Consiliului va stabili o dată pentru eliminarea controalelor la frontierele interne. Până la acea dată, se mențin anumite restricții privind utilizarea SIS.
- Cipru nu are încă acces la SIS.

Datele din SIS II pot fi căutate online (sub rezerva unor norme stricte de protecție a datelor) 24/7 prin intermediul birourilor SIRENE, la punctele de control la frontiere, pe teritoriul național și în străinătate în consulate. Datele sunt denumite alerte, o alertă fiind un set de date care permite autorităților să identifice **persoane**, de exemplu cetățeni europeni și cetățeni din afara UE, sau **obiecte**, pentru a lua măsuri corespunzătoare pentru combaterea criminalității și a imigrației neregulate.

Personalul Europolului autorizat special are dreptul, în limitele mandatului propriu, să acceseze și să consulte direct datele introduse în SIS II și poate solicita informații suplimentare din partea statului membru vizat.

Membrii naționali ai Eurojustului și asistenții acestora au dreptul, în limitele mandatului lor, să acceseze și să consulte datele introduse în SIS II.

Potrivit articolului 47 din CAAS, ofițerii de legătură detașați în cadrul autorităților polițienești din alte state Schengen sau țări terțe sunt responsabili de schimbul de informații în temeiul:

- articolului 39 alineatele (1), (2) și (3) în conformitate cu dreptul intern, în scopul prevenirii și depistării infracțiunilor;
- articolului 46, chiar și din proprie inițiativă, în scopul prevenirii infracțiunilor și amenințărilor la adresa ordinii și securității publice.

⁵⁷ Decizia 2010/365/UE a Consiliului din 29 iunie 2010 privind aplicarea dispozițiilor acquis-ului Schengen referitoare la Sistemul de informații Schengen în Republica Bulgaria și în România, JO L 166/17, 1.7.2010

⁵⁸ Decizia (UE) 2017/733 a Consiliului din 25 aprilie 2017 privind aplicarea dispozițiilor acquis-ului Schengen referitoare la Sistemul de informații Schengen în Republica Croația, JO L 108/31, 26.4.2017

Ar trebui remarcat faptul că dispozițiile articolului 39 alineatele (1), (2) și (3) și ale articolului 46, în măsura în care se referă la schimbul de informații și de date operative cu privire la criminalitatea gravă, se înlocuiesc cu cele din Decizia-cadru 2006/960/JAI a Consiliului, „Decizia-cadru suedeză”. Cu toate acestea, dispozițiile articolului 39 alineatele (1), (2) și (3) și ale articolului 46 se aplică în continuare cu privire la infracțiunile pasibile de o pedeapsă cu închisoarea mai mică de 12 luni.

3.3. Europol

Legislație

Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului, JO L 135, 24.5.2016, p. 53-114 (aplicabil începând cu 1 mai 2017).

Dispoziții-cheie

Obiectivul Europolului este acela de a sprijini și consolida acțiunea autorităților competente ale statelor membre responsabile cu prevenirea și combaterea criminalității, precum și cooperarea reciprocă a acestora în vederea prevenirii și combaterii criminalității organizate, a terorismului și a altor forme grave de criminalitate care afectează două sau mai multe state membre. În acest scop, Europolul colectează, stochează, prelucerează, analizează și face schimb de informații și date operative în materie penală.

Fiecare stat membru desemnează o unitate națională (ENU) care funcționează ca organism de legătură între Europol și autoritățile competente din statele membre. Unitățile naționale Europol efectuează sarcini legate de schimbul de informații și date operative pertinente. Fiecare unitate națională detașează cel puțin un ofițer de legătură care constituie biroul național de legătură la Europol și care reprezintă interesele unității naționale. Ofițerii de legătură sunt însărcinați cu partajarea de informații, pe de o parte, între statele membre și Europol și, pe de altă parte, la nivel bilateral, între alte țări. Aceste schimburi bilaterale pot să privească infracțiuni din afara mandatului Europolului.

Regulamentul Europol introduce un nou concept pentru prelucrarea datelor, care este denumit în mod obișnuit conceptul de gestionare integrată a datelor (IDMC). IDMC poate fi definit ca fiind posibilitatea de a utiliza informații legate de infracțiuni în scopuri profesionale multiple, astfel cum o indică proprietarul datelor, permițând gestionarea și prelucrarea acestora într-un mod integrat și neutru din punct de vedere tehnologic. În temeiul Deciziei Europol a Consiliului, prelucrarea datelor a fost structurată în jurul sistemelor. Regulamentul Europol nu mai conține trimiteri la sisteme, în schimb impune indicarea scopurilor prelucrării. Pentru a se facilita o tranziție fără probleme, utilizatorii pot continua să lucreze cu sistemele existente într-un mod care să respecte noul cadru juridic.

Unitatea națională răspunde de comunicarea cu sistemul informațional Europol (EIS) utilizat pentru prelucrarea datelor necesare îndeplinirii sarcinilor care revin Europolului. Unitatea națională, ofițerii de legătură și personalul Europolului autorizat în mod corespunzător au dreptul de a introduce date în sisteme și să extragă date din acestea. Informațiile introduse în EIS sunt în general considerate ca fiind furnizate în scopul verificării încrucișate [articolul 18 alineatul (2) din regulament] și al analizei strategice/tematice [articolul 18 alineatul (2) litera (b) din regulament].

3.4. Interpol

Legislație

Constituția Interpolului⁵⁹

Normele care reglementează prelucrarea informațiilor⁶⁰

Norme privind controlul informațiilor și accesul la dosarele Interpol

Dispoziții-cheie

Misiunea Interpol este de a facilita cooperarea polițienească internațională în vederea prevenirii și combaterii criminalității prin intermediul unei cooperări sporite și al inovării în materie de poliție și de securitate. Se iau măsuri în limitele legilor existente în statele membre și în spiritul Declarației universale a drepturilor omului. Fiecare dintre cele 190 de state membre are un birou central național (BCN), cu personal format din funcționari însărcinați cu aplicarea legii, cu o înaltă calificare, din statul membru respectiv.

Constituția Interpol este un acord internațional care confirmă, în calitate de membri, guvernele tuturor țărilor care au participat la adoptarea acesteia în 1956 și stabilește procedura de candidatură pentru a adera la Interpol pentru țările care nu erau membri în 1956.

Ca principal document juridic, Constituția stabilește scopurile și obiectivele Interpolului. Aceasta stabilește mandatul organizației pentru a asigura cea mai amplă cooperare posibilă între toate autoritățile de poliție judiciară și pentru a reprimă infracțiunile de drept comun.

În afara Constituției, o serie de texte fundamentale constituie cadrul juridic al Interpolului. Au fost create o serie de niveluri de control pentru a asigura respectarea normelor. Acestea se referă la controalele efectuate de birourile centrale naționale (BCN), de secretariatul general și de organismul independent de monitorizare, cunoscut sub denumirea de Comisia pentru monitorizarea dosarelor Interpol.

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. Ofițerii de legătură

Legislație

Articolul 47 din Convenția de punere în aplicare a Acordului Schengen din 19 iunie 1990 (CAAS)⁶¹

Decizia 2003/170/JAI a Consiliului din 27 februarie 2003 privind folosirea comună a ofițerilor de legătură detașați de autoritățile de aplicare a legii din statele membre⁶².

Decizia 2006/560/JAI a Consiliului din 24 iulie 2006 de modificare a Deciziei 2003/170/JAI privind folosirea comună a ofițerilor de legătură detașați de autoritățile de aplicare a legii din statele membre⁶³

Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului, JO L 135, 24.5.2016, p. 53-114 (aplicabil începând cu 1 mai 2017).

Decizia 2008/615/JAI a Consiliului privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, JO L 210/1, 6.8.2008

Acorduri bilaterale

⁶¹ Convenția de punere în aplicare a Acordului Schengen din 19 iunie 1990 (CAAS), JO L 239/19, 22.9.2000.

⁶² Decizia 2003/170/JAI a Consiliului din 27 februarie 2003, JO L 67/27, 12.3.2003.

⁶³ Decizia 2006/560/JAI a Consiliului din 24 iulie 2006, JO L 219/31, 10.8.2006.

Dispoziții-cheie

Articolul 47 din CAAS prevede că statele membre „pot încheia acorduri bilaterale privind detașarea, pentru o perioadă determinată sau nedeterminată, de ofițeri de legătură aparținând [unui stat membru] pe lângă autoritățile de poliție ale [altor state membre]”. Ofițerii de legătură nu sunt împuterniciți să execute măsuri polițienești în mod autonom, iar articolul 47 precizează că astfel de detașări au „ca scop să avanseze și să accelereze cooperarea [...], în special prin acordarea de asistență:

- a) sub forma schimbului de informații pentru combaterea criminalității, atât prin prevenire cât și prin aplicarea legii;
- b) la realizarea cererilor de asistență reciprocă pe linie de activități polițienești și judiciare în probleme penale;
- c) în legătură cu sarcinile autorităților responsabile cu supravegherea frontierelor externe”.

Mai multe informații despre astfel de detașări pot fi găsite în „Manualul de fotbal”⁶⁴ și în Recomandarea Consiliului din 6 decembrie 2007 privind un manual pentru autoritățile polițienești și de securitate privind cooperarea cu ocazia evenimentelor majore care au o dimensiune internațională⁶⁵.

Dispoziția din CAAS conform căreia ofițerii naționali de legătură pot reprezenta interesele unuiu sau a mai multor alte state membre a fost dezvoltată de Decizia Consiliului privind folosirea comună a ofițerilor de legătură detașați de autoritățile de aplicare a legii din statele membre (modificată în 2006). S-a prevăzut, de asemenea, îmbunătățirea cooperării dintre ofițerii de legătură din diferite state membre la locul lor de detașare. S-a subliniat în numeroase foruri că această cooperare ar trebui încurajată.

⁶⁴ Rezoluția Consiliului din 3 iunie 2010 privind un manual actualizat de recomandări pentru cooperarea polițienească internațională și de măsuri pentru prevenirea și ținerea sub control a violenței și dezordinii legate de meciurile de fotbal de anvergură internațională care implică cel puțin un stat membru, JO C 165/1, 24.6.2010.

⁶⁵ JO C 314/4, 22.12.2007.

În conformitate cu Regulamentul Europol, fiecare stat membru desemnează o unitate națională (ENU) care funcționează ca organism de legătură între Europol și autoritățile competente ale statelor membre responsabile de prevenirea și combaterea infracțiunilor. Unitățile naționale Europol efectuează sarcini legate de schimbul de informații și date operative pertinente. Fiecare unitate națională detașează cel puțin un ofițer de legătură care constituie biroul național de legătură la Europol și care reprezintă interesele unității naționale. Ofițerii de legătură sunt însărcinați cu partajarea de informații între, pe de o parte, unitatea națională și Europol și, pe de altă parte, la nivel bilateral, între alte unități naționale. Aceste schimburi bilaterale pot să privească infracțiuni din afara mandatului Europolului.

Decizia 2008/615/JAI a Consiliului („Decizia Prüm”) prevede la articolele 17 și 18 detașarea funcționarilor naționali, în scopul menținerii ordinii și securității publice și al prevenirii infracțiunilor.

3.6. Schimbul de date în temeiul Deciziei Prüm

Legislație

- Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere
- Decizia 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008)

Dispoziții-cheie

Statele membre își acordă reciproc acces online transfrontalier la datele de referință din fișierele naționale de date ADN desemnate și din sistemele automatizate de identificare dactiloscopică (AFIS), precum și la datele privind înmatricularea vehiculelor (VRD) (a se vedea capitolul 2 din Decizia 2008/615/JAI a Consiliului).

În fiecare stat membru trebuie desemnate puncte de contact naționale specifice. Legislația națională trebuie să prevadă în mod corespunzător dispoziții privind protecția și securitatea datelor.

Compararea automatizată a profilurilor biometrice anonime se bazează pe un sistem de tip „hit/no hit” (răspuns pozitiv/negativ), cu excepția cazului VRD în care se afișează în mod automat proprietarul/deținătorul datelor căutate.

În cazul unei concordanțe biometrice, PCN al statului membru care efectuează căutarea primește, în cadrul unui proces automatizat, datele de referință în raport cu care a fost găsită concordanța.

Anumite date cu caracter personal suplimentare și alte informații în legătură cu datele de referință pot fi solicitate ulterior prin intermediul unor proceduri de asistență reciprocă, inclusiv al celor adoptate în temeiul „Deciziei-cadru suedeze”.

Furnizarea unor astfel de date suplimentare este reglementată de dreptul național al statului membru solicitat, inclusiv de dispozițiile privind asistența judiciară. Este de la sine înțeles faptul că furnizarea de date cu caracter personal necesită un nivel adecvat de protecție a datelor din partea statului membru destinatar⁶⁶.

Pentru prevenirea infracțiunilor și în interesul menținerii ordinii și a securității publice în cazul unor evenimente majore care au o dimensiune transfrontalieră, statele membre pot, fie la cerere, fie din proprie inițiativă, să își furnizeze reciproc date fără caracter personal, precum și date cu caracter personal. În acest scop, sunt desemnate puncte de contact naționale (PCN) (a se vedea capitolul 3 din Decizia 2008/615/JAI a Consiliului).

În vederea prevenirii infracțiunilor de terorism, statele membre își pot furniza reciproc date cu caracter personal în anumite circumstanțe. În acest scop, sunt desemnate puncte de contact naționale specifice (a se vedea capitolul 4 din Decizia 2008/615/JAI a Consiliului).

⁶⁶ Decizia 2008/615/JAI respectă nivelul de protecție stabilit pentru prelucrarea datelor cu caracter personal în cadrul Convenției Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, al Protocolului său adițional din 8 noiembrie 2001 și în principiile Recomandării nr. R (87) 15 a Consiliului Europei de reglementare a utilizării datelor cu caracter personal în domeniul polițienesc.

3.7. Sistemul de informații privind vizele (VIS)

Legislație

Decizia Consiliului din 8 iunie 2004 de instituire a Sistemului de informații privind vizele (VIS) (2004/512/CE), JO L 213/5, 15.6.2004

Decizia 2013/392/UE a Consiliului de stabilire a datei de la care produce efecte Decizia 2008/633/JAI privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave, JO 2013 L 198, p. 45

Dispoziții-cheie

VIS este un sistem care permite autorităților naționale competente să introducă și să actualizeze date privind vizele și să consulte aceste date pe cale electronică. VIS se bazează pe o structură centralizată și este format dintr-un sistem informatic central, sistemul central de informații privind vizele (CS-VIS), o interfață națională în fiecare stat membru (NI-VIS) și infrastructura de comunicații dintre CS-VIS și NI-VIS.

La 16 aprilie 2015, Curtea de Justiție a anulat Decizia 2013/392/UE a Consiliului de stabilire a datei de la care produce efecte Decizia 2008/633/JAI privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave. Cu toate acestea, Curtea a precizat că efectele Deciziei 2013/392 sunt menținute până la intrarea în vigoare a unui nou act destinat să o înlocuiască.

3.8. Eurodac

Legislație

Eurodac este un sistem informatic cu scopul inițial de a facilita aplicarea efectivă a Convenției de la Dublin. Convenția de la Dublin, semnată la 15 iunie 1990, a fost înlocuită de Regulamentul (CE) nr. 343/2003 al Consiliului din 18 februarie 2003 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe.

În urma modificărilor aduse regulamentelor privind Eurodac, acestea au fost reformate prin Regulamentul nr. 603/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid și privind cererile autorităților de aplicare a legii din statele membre și ale Europol de comparare a datelor Eurodac în scopul asigurării respectării aplicării legii și de modificare a Regulamentului (UE) nr. 1077/2011 de instituire a Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (reformare) (JO L 180/1, 29.6.2013).

Dispoziții-cheie

Regulamentul nr. 603/2013 stabilește scopul Eurodacului și definește condițiile de accesare de către autoritățile naționale de aplicare a legii desemnate și de către Europol a datelor Eurodacului în scopul prevenirii, depistării sau investigării infracțiunilor de terorism⁶⁷ sau a altor infracțiuni grave⁶⁸.

⁶⁷ Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164/3, 22.6.2002).

⁶⁸ Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO L 190/1, 18.7.2002).

3.9. Napoli II

Legislație

Actul Consiliului din 18 decembrie 1997 de elaborare, în baza articolului K.3 din Tratatul privind Uniunea Europeană, a Convenției cu privire la asistența reciprocă și cooperarea între administrațiile vamale, publicat în JO C 24/1 23.1.1998

Dispoziții-cheie

Statele membre se asistă reciproc pentru a preveni și a depista încălcările dispozițiilor vamale naționale și pentru a urmări în justiție și a sancționa încălcările dispozițiilor vamale comunitare și naționale. În cadrul investigațiilor penale, Convenția Napoli II stabilește proceduri conform cărora administrațiile vamale pot acționa în comun și face schimb de informații, din proprie inițiativă sau la cerere, privind activitățile de trafic ilicit.

Cererile sunt transmise în scris, într-una dintre limbile oficiale ale statului membru al autorității solicitate sau într-o limbă acceptată de autoritatea respectivă. Un formular stabilește standardul în ceea ce privește comunicarea de informații. Autoritățile implicate comunică toate informațiile care pot ajuta la prevenirea, detectarea și urmărirea penală a încălcărilor. Acestea fac schimb de date cu caracter personal, adică toate informațiile privind o persoană fizică identificată sau identificabilă.

Pentru a oferi asistența cerută, autoritatea solicitată sau autoritatea competentă căreia aceasta din urmă i se adresează procedează ca și când ar acționa pe cont propriu sau la cererea altei autorități din propriul stat membru.

3.9.1. Sistemul de informații al vămilor - SIV⁶⁹

Sistemul de informații al vămilor completează Convenția Napoli II⁷⁰. Sistemul centralizat de informații este gestionat de Comisie și vizează consolidarea administrației vamale a statelor membre prin schimbul rapid de informații în vederea prevenirii, investigării și urmăririi penale a încălcărilor grave ale dreptului național și comunitar. De asemenea, SIV creează o bază de date pentru identificarea dosarelor vamale (FIDE) pentru a sprijini investigațiile vamale.

Autoritățile desemnate de statele membre⁷¹ au acces direct la datele conținute în SIV. Pentru a consolida complementaritatea cu Europolul și Eurojustul, ambelor organisme le este garantat accesul limitat la citirea datelor din SIV și FIDE.

SIV cuprinde date cu caracter personal cu referire la mărfuri, mijloace de transport, întreprinderi, persoane, bunuri și mijloace bănești reținute, sub sechestru sau confiscate. Datele cu caracter personal nu pot fi copiate din SIV decât pe alte sisteme de prelucrare a datelor în vederea analizelor operaționale sau de gestionare a riscului, la care pot avea acces numai analiștii desemnați de statele membre.

FIDE permite autorităților naționale responsabile de efectuarea anchetelor vamale ca, în momentul în care deschid un dosar de anchetă, să identifice alte autorități care ar fi putut ancheta o anumită persoană sau întreprindere.

⁶⁹ Decizia 2009/917/JAI a Consiliului din 30 noiembrie 2009 privind utilizarea tehnologiei informației în domeniul vamal, JO L 323/20, 10.12.2009.

⁷⁰ Convenție redactată în baza articolului K.3 din Tratatul privind Uniunea Europeană, cu privire la asistența reciprocă și cooperarea între administrațiile vamale, JO C 24/2, 23.1.1998.

⁷¹ Punerea în aplicare a articolului 7 alineatul (2) și a articolului 8 alineatul (3) din Decizia 2009/917/JAI a Consiliului din 30 noiembrie 2009 privind utilizarea tehnologiei informației în domeniul vamal – liste actualizate ale autorităților competente, documentul 13394/11 ENFOCUSTOM 85.

3.10. Birourile naționale de recuperare a activelor (ARO) și CARIN

Legislație

Decizia 2007/845/JAI a Consiliului din 6 decembrie 2007 privind cooperarea dintre oficiile de recuperare a creanțelor din statele membre în domeniul urmăririi și identificării produselor provenite din săvârșirea de infracțiuni sau a altor bunuri având legătură cu infracțiunile, JO L 332/103, 18.12.2007.

Rețeaua Camden Inter-agenții de Recuperare a Bunurilor (CARIN) a fost înființată la Haga la 22-23 septembrie 2004 de Austria, Belgia, Germania, Irlanda, Țările de Jos și Regatul Unit.

Dispoziții-cheie

În urma adoptării Deciziei 2007/845/JAI a Consiliului⁷², toate statele membre au instituit sau desemnat între timp birouri de recuperare a activelor (ARO). Acestea pot face schimb direct de informații cu privire la aspectele legate de recuperarea activelor prin sistemul SIENA. Sub auspiciile Comisiei Europene și Europolului, rețeaua ARO facilitează cooperarea dintre birourile de recuperare a activelor din statele membre, precum și discuțiile strategice și schimbul de bune practici. Biroul Europolului privind activele provenite din săvârșirea de infracțiuni (ECAB) acționează ca punct focal pentru recuperarea activelor în interiorul UE.

Dispozițiile prevăzute în Directiva 2014/42/UE a Parlamentului European și a Consiliului din 3 aprilie 2014 privind înghețarea și confiscarea instrumentelor și produselor infracțiunilor săvârșite în Uniunea Europeană⁷³ vor spori suplimentar eficiența cooperării dintre birourile de recuperare a activelor în cadrul Uniunii Europene. Statelor membre li se solicită să transpună directiva până la data de 4 octombrie 2016.

⁷² Decizia 2007/845/JAI a Consiliului din 6 decembrie 2007 privind cooperarea dintre oficiile de recuperare a creanțelor din statele membre în domeniul urmăririi și identificării produselor provenite din săvârșirea de infracțiuni sau a altor bunuri având legătură cu infracțiunile, JO L 332/103, 18.12.2007.

⁷³ Directiva 2014/42/UE a Parlamentului European și a Consiliului din 3 aprilie 2014 privind înghețarea și confiscarea instrumentelor și produselor infracțiunilor săvârșite în Uniunea Europeană, JO L 127/39, 29.4.2014.

Rețeaua Camden Inter-agenții de Recuperare a Bunurilor (CARIN), înființată în 2004 pentru a sprijini identificarea, înghețarea, sechestrarea și confiscarea de bunuri legate de infracțiuni, la nivel transfrontalier, sporește schimbul reciproc de informații privind diferitele abordări naționale a căror sferă de aplicare se întinde în afara UE.

Începând din 2015, Rețeaua CARIN cuprinde specialiști din 53 de jurisdicții și 9 organizații internaționale, care servesc drept puncte de contact în scopul schimbului transfrontalier rapid de informații, la cerere sau din proprie inițiativă. ARO naționale cooperează între ele sau cu alte autorități care facilitează urmărirea și identificarea produselor provenite din săvârșirea de infracțiuni. Deși toate statele membre au înființat un ARO, există diferențe majore între statele membre în ceea ce privește structura organizațională, resursele și activitățile.

Schimbul de informații se poate realiza în conformitate cu dispozițiile privind protecția datelor ale statelor membre destinate și face obiectul aceluiași norme privind protecția datelor ca și când informațiile ar fi fost colectate în statul membru destinat. Trebuie promovat schimbul de informații spontan, în conformitate cu această decizie, aplicarea procedurilor și a termenelor prevăzute în Decizia-cadru suedeză.

3.11. Unitățile de informații financiare (FIU)

Legislație

Decizia 2000/642/JAI a Consiliului din 17 octombrie 2000 privind acordurile de cooperare între unitățile de informații financiare ale statelor membre în ceea ce privește schimbul de informații

JO L 271/4, 24.1.2000

Directiva (UE) 2015/849 a Parlamentului European și a Consiliului din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului și de abrogare a Directivei 2005/60/CE a Parlamentului European și a Consiliului și a Directivei 2006/70/CE a Comisiei

JO L 141/73, 5.6.2015

Dispoziții-cheie

O solicitare trebuie să specifice modul în care se vor utiliza informațiile solicitate și – un aspect esențial al deciziei – FIU care răspunde trebuie să furnizeze toate informațiile pertinente, inclusiv informații financiare și date în materie de aplicare a legii. Cu toate acestea, o FIU poate refuza să divulge informații în cazul în care acestea ar aduce atingere unei investigații penale în curs sau ar fi în mod clar disproporționate față de interesele legitime ale subiectului în cauză sau nu ar respecta în orice alt mod principiile fundamentale de drept intern.

FIU trebuie să ia toate măsurile necesare, inclusiv măsuri de securitate, pentru a garanta că nicio altă autoritate, agenție sau serviciu nu are acces la informațiile transmise. Statele membre prevăd și aprobă canale corespunzătoare și protejate de comunicare între FIU.

FIU.NET este o rețea informatică descentralizată pentru schimbul de informații între FIU.

FIU.NET, menită inițial să consolideze poziția unităților de informații financiare, s-a dezvoltat în ultimii ani dintr-un instrument securizat elementar pentru schimbul structurat, bilateral de informații într-un instrument securizat multifuncțional pentru schimbul de informații multilateral, cu funcții de gestionare a cazurilor, precum și de standardizare semiautomată a proceselor. În cadrul FIU.NET, fiecare caracteristică nouă și fiecare proces automat sunt opționale, neexistând o obligație în acest sens. Unitățile individuale de informații financiare pot decide ce posibilități și caracteristici oferite de FIU.NET să utilizeze, utilizând numai caracteristicile pe care le agreează și excluzându-le pe cele de care nu au nevoie sau pe care nu doresc să le utilizeze.

3.12. Acordul UE-SUA privind Programul de urmărire a finanțărilor în scopuri teroriste (TFTP)

Legislație

Acordul dintre Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste

JO L 195/5, 27.7.2010

Dispoziții-cheie

În perioada următoare 9/11, UE și SUA au decis să colaboreze strâns și au încheiat Acordul privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite în cadrul Programului de urmărire a finanțărilor în scopuri teroriste (Acordul TFTP UE-SUA). În conformitate cu acordul, Departamentul de Trezorerie al SUA pune, de asemenea, informații TFTP la dispoziția autorităților din domeniile aplicării legii, securității publice sau combaterii terorismului din statele membre vizate sau, după caz, la dispoziția Europolului și Eurojustului.

TFTP este echipat cu măsuri solide de control pentru a se asigura că sunt respectate garanțiile, inclusiv cele privind protecția datelor cu caracter personal. Datele sunt prelucrate exclusiv în scopul prevenirii, investigării, depistării sau urmăririi penale a actelor de terorism sau a finanțării acestora.

În sensul acordului, Departamentul de Trezorerie al SUA poate solicita date de mesagerie financiară în materie de plăți și date conexe stocate pe teritoriul UE din partea furnizorilor desemnați ai serviciilor internaționale de mesagerie financiară în materie de plăți.

Beneficiile rezultate din datele TFTP pentru statele membre, Europol și Eurojust sunt limitate de faptul că analiza TFTP a plăților transfrontaliere se bazează exclusiv pe mesaje FIN (transfer între instituții financiare), un tip de mesaj SWIFT prin care informațiile financiare sunt transmise de la o instituție financiară la alta. Alte metode de plată nu sunt luate în considerare. Cu toate acestea, acordul TFTP este singurul mecanism care permite, într-un interval de timp foarte scurt, cartografierea și elaborarea de profiluri ale tranzacțiilor suspectate a fi legate de terorism sau de finanțarea terorismului, în vederea consolidării securității interne.

Datorită unei mai mari conștientizări a clauzelor de reciprocitate din acest acord, autoritățile din UE aplică din ce în ce mai mult acest mecanism pentru a beneficia de schimburile de date cu SUA. Ar trebui observat, în acest context, că toate solicitările din partea autorităților din UE de căutări în TFTP trebuie să îndeplinească cerințele prevăzute la articolul 10 din acord.

Deși acordul nu prevede ca statele membre să solicite prin intermediul Europolului o căutare de informații relevante obținute prin intermediul TFTP, ar fi util, în vederea îmbunătățirii reacției UE la terorism și la finanțarea acestuia, ca statele membre să informeze cel puțin Europolul în mod sistematic și în timp util cu privire la solicitările lor directe în temeiul articolului 10. Pentru a sprijini statele membre în direcționarea solicitărilor de căutări în TFTP, Europolul a creat un punct unic de contact (SPOC) și, grație mediului său bazat pe fișiere de lucru pentru analiză (AWF) și cooperării bine stabilite cu Trezoreria, se află într-o poziție favorabilă pentru a trata în mod eficient solicitările statelor membre.

3.13. Schimbul de informații cu privire la cazierele judiciare (ECRIS)

Legislație

Decizia-cadru 2009/315/JAI a Consiliului din 26 februarie 2009 privind organizarea și conținutul schimbului de informații extrase din cazierele judiciare între statele membre, JO L 93, 7.4.2009, p.23. Această decizie-cadru abrogă Decizia 2005/876/JAI a Consiliului din 21 noiembrie 2005 privind schimbul de informații extrase din cazierul judiciar, JO L 322/33, 9.12.2005, p. 33.

Decizia 2009/316/JAI a Consiliului de instituire a Sistemului european de informații cu privire la cazierele judiciare (ECRIS) în aplicarea articolului 11 din Decizia-cadru 2009/315/JAI se întemeiază pe principiile stabilite de Decizia-cadru 2009/315/JAI și aplică și completează respectivele principii din punct de vedere tehnic.

Dispoziții-cheie

Decizia-cadru 2009/315/JAI a Consiliului obligă statul membru de condamnare să transmită, cât mai curând posibil, orice condamnare introdusă în cazierul său judiciar statului (statelor) membru (membre) de cetățenie al(e) persoanei respective, precum și orice modificare sau ștergere realizată în legătură cu condamnarea respectivă. Statul membru de cetățenie este obligat să stocheze informațiile în scopul retransmiterii acestora și orice modificare sau ștergere efectuată în statul membru de condamnare atrage o modificare sau ștergere identică în cazierul judiciar din statul de cetățenie al persoanei vizate. În cazul în care se solicită informații referitoare la condamnări în scopul unor proceduri penale din statul membru de cetățenie, statul membru solicitat are obligația de a transmite informațiile privind condamnările stocate în cazierul judiciar. În cazul în care se solicită informații în alte scopuri decât procedurile penale, statul membru solicitat răspunde în conformitate cu dreptul național.

Decizia 2009/316/JAI a Consiliului definește modalitățile prin care un stat membru trebuie să transmită astfel de informații. Decizia Consiliului stabilește cadrul pentru un sistem computerizat de schimb de informații extrase din cazierele judiciare. Autoritățile centrale din fiecare stat membru utilizează formularele speciale de solicitare și de răspuns anexate la decizia-cadru, prin intermediul modalității electronice descrise în legislație.

3.14. Păstrarea datelor referitoare la telecomunicații

Legislație

Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE⁷⁴.

⁷⁴ Hotărârea Curții de Justiție a Uniunii Europene din 8 aprilie 2014 a declarat nulă directiva.

Dispoziții-cheie

Directiva se aplică furnizorilor de servicii de comunicații electronice. Directiva prevede că furnizorii ar trebui să păstreze datele de transfer și de localizare, precum și datele conexe necesare pentru identificarea abonatului sau a utilizatorului, pentru a comunica aceste date autorităților naționale competente la cererea acestora. În vederea investigării, depistării și urmăririi penale a infracțiunilor grave, statele membre obligă furnizorii de servicii de comunicații electronice sau de rețele de comunicații publice să păstreze categoriile de date necesare pentru a identifica:

- sursa unei comunicații
- destinația unei comunicații
- data, ora și durata unei comunicații
- tipul unei comunicații
- echipamentul de comunicație al utilizatorilor sau ceea ce se susține că este echipamentul acestora
- localizarea echipamentului de comunicație mobilă.

Nu pot fi păstrate date care dezvăluie conținutul comunicației.

3.15. Directiva privind PNR (registrul cu numele pasagerilor)

Legislație

Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave.

Dispoziții-cheie

Directiva stabilește, la nivelul Uniunii, un cadru juridic comun pentru transferul și prelucrarea datelor din PNR și prevede:

- b) transferul de către transportatorii aerieni⁷⁵ al datelor din registrul cu numele pasagerilor (PNR) privind pasagerii zborurilor extra-UE. În cazul în care un stat membru decide să aplice directiva zborurilor intra-UE, toate dispozițiile se aplică zborurilor intra-UE ca și cum ar fi zboruri extra-UE;
- c) prelucrarea datelor din PNR, inclusiv colectarea, utilizarea și păstrarea acestora de către statele membre și schimbul de astfel de date între statele membre.

În scopul prelucrării datelor din PNR, fiecare stat membru instituie sau desemnează o autoritate competentă care să acționeze ca unitate de informații despre pasageri (UIP). Două sau mai multe state membre pot institui sau desemna o singură autoritate în calitatea de UIP comună.

⁷⁵ Directiva nu aduce atingere posibilității statelor membre de a prevedea, în dreptul intern, un sistem pentru colectarea și prelucrarea datelor din PNR de la operatorii economici care nu sunt transportatori aerieni, cum ar fi agențiile de voiaj și operatorii de turism care oferă servicii legate de călătorii – inclusiv rezervarea de zboruri – pentru care colectează și prelucrează date din PNR, sau de la alți transportatori decât cei menționați în directivă, cu condiția ca aceste dispoziții ale dreptului intern să respecte dreptul Uniunii.

Datele din PNR, care sunt prevăzute în anexa I la directivă, urmează să fie transferate la UIP-uri în măsura în care acestea sunt deja colectate de către transportatorii aerieni în cursul activităților lor obișnuite. Unii transportatori păstrează informații prealabile referitoare la pasageri (API) ca parte a datelor din PNR, iar alții nu. Indiferent de modul în care transportatorii aerieni colectează API, aceștia trebuie să transfere datele API la UIP, care le vor prelucra în același mod în care prelucrează datele din PNR. Anexa II la directivă conține o listă de „infrațiuni grave” care intră sub incidența directivei.

Prelucrarea datelor din PNR servește la evaluarea pasagerilor înainte de sosirea acestora într-un stat membru sau de plecarea acestora dintr-un stat membru, în vederea identificării persoanelor care necesită o examinare suplimentară de către autoritățile competente, în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave, și, după caz, de către Europol, în limitele competențelor sale și în vederea îndeplinirii sarcinilor sale.

Pentru a efectua evaluarea, UIP pot

(a) să compare datele din PNR cu bazele de date relevante în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave, inclusiv cu bazele de date privind persoane sau obiecte căutate sau care fac obiectul unei alerte, în conformitate cu normele Uniunii și cu normele internaționale și naționale aplicabile unor astfel de baze de date, sau

(b) să prelucreze date din PNR în conformitate cu anumite criterii prestabilite.

La nivel național, UIP transmit datele din PNR sau rezultatul prelucrării acestora către autoritățile naționale de aplicare a legii competente care au dreptul de a examina în continuare dosarul sau de a adopta măsuri adecvate pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave. Cu toate că UIP constituie principalul canal de schimb de informații la nivel transfrontalier, autoritățile competente se pot adresa în mod direct unităților de informații despre pasageri din alte state membre în caz de urgență și în condiții bine definite.

La nivelul Uniunii, UIP fac schimb deopotrivă de date din PNR colectate de la transportatorii aerieni și de rezultatele prelucrării datelor respective, între ele și cu Europol, care are dreptul, în limitele competențelor sale și în vederea desfășurării sarcinilor sale, să solicite astfel de date de la UIP.

Datele din PNR sunt păstrate într-o bază de date la UIP pentru o perioadă de cinci ani după transferul lor din statul membru de sosire sau de plecare a zborului. Cu toate acestea, toate datele din PNR sunt depersonalizate după o perioadă de șase luni. Acest lucru se realizează prin mascarea oricăror elemente de date care ar putea servi la identificarea directă a pasagerului la care se referă datele respective. Lista datelor din PNR care trebuie să fie mascate este prevăzută în directivă. După cinci ani, datele din PNR trebuie șterse, cu excepția cazului în care au fost transferate unei autorități competente în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave, în acest caz păstrarea datelor fiind reglementată de dreptul intern.

În conformitate cu legislația UE privind protecția datelor, Directiva privind PNR interzice prelucrarea datelor sensibile, precum cele privind rasa sau originea etnică, opiniile politice, religia sau convingerile filozofice, apartenența la un sindicat, sănătatea, viața sexuală sau orientarea sexuală.

3.16. Informații prelabile privind pasagerii (API)

Legislație

Directiva 2004/82/CE a Consiliului din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii

Dispoziții-cheie

Directiva are drept scop îmbunătățirea controalelor la frontieră și combaterea imigrației ilegale. În acest scop, directiva impune statelor membre să stabilească obligația transportatorilor aerieni de a comunica anumite informații privind propriii pasageri înainte de intrarea acestora pe teritoriul Uniunii Europene. Aceste informații sunt denumite informații prelabile privind pasagerii (API). În anumite condiții și circumstanțe, statele membre pot de asemenea utiliza date API în scopul aplicării legii.

Informațiile sunt furnizate la cererea autorităților responsabile cu efectuarea controlului persoanelor la frontierele externe ale UE.

Transportatorii aerieni ar trebui să transmită datele API pe cale electronică sau, în caz de eșec, prin orice alt mijloc adecvat, autorităților care efectuează controale la punctul de frontieră prin care pasagerul intră pe teritoriul UE. Datele API sunt confruntate cu bazele de date naționale și europene, cum ar fi Sistemul de Informații Schengen (SIS) și Sistemul de informații privind vizele (VIS).

Atunci când datele API corespund unui element dintr-o bază de date, se transmite o alertă poliției de frontieră, iar pasagerul în cauză este vizat pentru examinare la sosire.

Datele API colectate și transmise trebuie șterse de către transportatori și autorități în termen de 24 de ore de la transmitere sau de la sosire. Cu toate acestea, autoritățile de frontieră pot să păstreze fișierele temporare pentru o perioadă mai lungă de 24 de ore în cazul în care datele sunt necesare ulterior în scopul exercitării funcțiilor statutare ale autorităților de frontieră sau pentru asigurarea respectării legilor și a reglementărilor privind intrarea și imigrația, inclusiv a dispozițiilor acestora privind protecția ordinii publice și a securității naționale.

3.17. Încălcăările normelor de circulație care afectează siguranța rutieră

Legislație

Directiva (UE) 2015/413 a Parlamentului European și a Consiliului din 11 martie 2015 de facilitare a schimbului transfrontalier de informații privind încălcările normelor de circulație care afectează siguranța rutieră, JO L 68/9

Dispoziții-cheie

Statele membre își acordă reciproc acces online la propriile date naționale privind înmatricularea vehiculelor (VRD), în vederea executării sancțiunilor pentru anumite încălcări ale normelor de circulație care afectează siguranța rutieră săvârșite cu un vehicul înmatriculat într-un alt stat membru decât statul membru în care a avut loc încălcarea. Statul membru în care s-a săvârșit încălcarea utilizează datele obținute în scopul de a stabili persoana responsabilă pentru încălcările normelor de circulație rutieră. Schimbul de informații se aplică în cazul:

- excesului de viteză
- nefolosirii centurii de siguranță
- nerespectării semnificației culorii roșii a semaforului
- conducerii sub influența alcoolului
- conducerii sub influența drogurilor
- nefolosirii căștii de protecție
- utilizării unei benzi interzise
- folosirii ilegale a unui telefon mobil sau a altor dispozitive de comunicare în timpul conducerii.

Utilizând aplicația informatică specifică EUCARIS, statele membre permit accesul reciproc la VRD al punctelor lor de contact naționale (PCN), cu competența de a efectua căutări automatizate cu privire la

- a) date privind vehiculele și
- b) date privind proprietarii sau deținătorii vehiculelor.