Council of the European Union

Brussels, 29 November 2024
(OR. en)

16064/24

IXIM 238
JAI 1725
COMIX 474

NOTE

From:	General Secretariat of the Council
To:	Working Party on JHA Information Exchange (IXIM)
No. prev. doc.:	5825/20
Subject:	Manual on Law Enforcement Information Exchange

Background

Following the discussions at IXIM WG during the Belgian Presidency, a structured approach was agreed upon to carry out a stocktaking exercise and to address the challenges, such as following up the developments on the legislative landscape, the questions related to the practical implementation of the Information Exchange Directive (IED), the outline of the methodologies, and streamline the implementation of the IED across Member States. Based on the outcome of these discussions, a new community has been established within the structure of the IXIM Working Party (Manual on Law Enforcement Information Exchange).

This community under the umbrella of the IXIM Working Party was established in a spirit of close collaboration. With the involvement of Member States' experts and the General Secretariat of the Council, it is a collective effort aimed at revising the existing Manual on Law Enforcement Information Exchange (5825/20) to better align with the current needs and practices of the Member States.

The Hungarian Presidency took proactive steps by convening two meetings (VTC) of the Manual on Law Enforcement Information Exchange community on 12 September and 22 October 2024. The Presidency collected all the proposals for modification from the Member States to create a comprehensive manual. During the discussions, it became clear, that some of the points and questions raised by delegates need to be addressed to the Commission, as they may pertain to the implementation of the new Directive, as opposed to the Manual on Law Enforcement Information Exchange itself. Another part of the Member States' proposals is to change the existing Manual's structure and content. Based on the conclusions of the meetings, the community has to define/revise:

- the content first,
- the structure second, and
- the fact sheets third, which also need to be upgraded, and the decision is necessary on its form (e.g., common catalogue/matrix).

In close cooperation with GSC, the Hungarian Presidency has started the work and prepared the first draft version of the revised Manual based on Member States' written contributions as a starting point for future work. Some areas are yet to be covered, which include the new EU Legislations, such as the Prüm II Regulation, the API Regulations, and the best practices after the entry into force of the IED.

Based on the results mentioned above, the Presidency has been focusing on revising the content, particularly those parts of the Manual that can be connected to the Information Exchange Directive and interoperability.

Parts have been revised

During the discussions in the meetings of the Manual on Law Enforcement Information Exchange community, the experts agreed that the content of the Manual should be revised first, particularly the references related to the Swedish Framework Decision throughout the text.

There were slight updates executed in Point 1.1, in line with the IED and Point 1.2. was simplified and shortened.

The experts agreed to incorporate COM's text suggestions regarding the Visa Information System (VIS), the Schengen Information System (SIS), the Eurodac, the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), and Common Identity Repository (CIR). Regarding VIS, the existing Point 2.6 has been upgraded, and new Points with the above mentioned updated content were created as follows:

- 2.7 SIS, (merging Points 2.1 and 2.7 still have to be discussed),
- 2.8. Eurodac, (Point 2.7 in previous version),
- 2.9 EES, (Point 2.11 in previous version),
- 2.10 ETIAS, (Point 2.12 in previous version),
- 2.11 CIR (COM suggestion as a new element, discuss where to add the other IO elements as well from the Interoperability point)

In Point 2.3 (SIENA), we have identified and outlined some minor adjustments that enhance the overall clarity and coherence of the content.

The references regarding the Data Protection Directive were also updated in 3.1 based on the written contributions provided by MSs, and the references in Figure 1 and Figure 2 were also eliminated.

Parts have to be revised during future work

- 1. Introduction
- 2. Purpose of the Manual
- 3. Content of the Manual
- 4. Way forward
- Table of content
- PART I: Operational Context
- PART II: 1.5 Prüm, the whole chapter has to be revised according to Prüm II Regulation at a later stage.
- PART II: 1.6 (NFIP); 1.7 (NFFP); 1.8 (PCCC); 1.9 (Liaison Officers); 1.10 (ARO); 1.11 (FIU); 1.12 (Naples II Convention); 1.13 (PIU); 1.14 (EES); 1.15 (ETIAS); 1.16 (Interoperability); 1.17 (Common channels).
- PART II: 2.1. (SIS II); 2.2 (EIS); 2.4 (Interpol's global police communications system); 2.5 (ECRIS); 2.8 (CIS); 2.9 (FADO); 2.10 (PRADO); 2.13 (Summary Overview of Information Systems used for EU Information Exchange). In the case of Points 2.8 – 2.10 and 2.13, a new sub-numbering has been created as 2.12 (CIS), 2.13 (FADO), 2.14 (PRADO) and 2.15 (Summary table).
- PART II: Points 3.3 - 3.22 - Content and structure have to be discussed.
- PART III: National factsheets

Practical examples at the end of some chapters (e.g. "Typical Structure of a National SPOC (Single Point of Contact) office"; "Examples of automated data exchange under the Prüm Council Decisions") are to determine whether to retain them, for instance, in the frame of a "Best practices" chapter.

Way forward

The ongoing revision of the Law Enforcement Information Exchange Manual is essential to ensure it remains up-to-date and enhances communication and collaboration among law enforcement agencies.

The possible way forward is explored in document 16296/24, providing insights for the next steps.

ANNEX

MANUAL ON LAW ENFORCEMENT INFORMATION EXCHANGE

1. Introduction

The Manual on Law Enforcement Information Exchange aims at complementing the Manual on cross-border operations (10505/4/09 REV 4). Both content and structure of the manual and the national fact sheets have been endorsed by DAPIX in the framework of the Information Management Strategy (IMS) for EU internal security in view of supporting, streamlining and facilitating cross-border information exchange.

In order to increase the practical value of the manual, translations in all official languages of the Union will be made available. Furthermore, the manual will be updated twice a year, as necessary in the light of new legislation or practical experience.

The national contact details are regularly updated by the Member States and set out in the national factsheets, which are issued as an addendum (ADD 1) to the manual. This addendum comprises sensitive information and cannot be disclosed without consulting the GSC in line with Regulation (EC) No 1049/2001[1].

2. Purpose of the manual

The manual is primarily intended as a tool for police officers working in the area of International Liaison and in particular for so-called '**SPOC' operators.** Accordingly, it should be as user-friendly and comprehensive as possible.

The manual aims to inform and facilitate **practical day-to-day cooperation** between different Member States' authorities involved in police information exchange at both national and international level, to serve training purposes and ensure that better informed decisions will be made when it comes to seeking and exchanging information across borders.

[1] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. The regulation lays down the general principles and limits on access.

The manual contains **an overview of all EU systems, legal bases and instruments of information exchange** available to the law enforcement authorities of the Member States. This way, the user is fully informed of the available options when it comes to deciding how to seek or provide information across borders.

National fact sheets complete the manual by setting out relevant contact details and information available for cross-border exchange. By regularly up-dating these sheets, Member States will have complied with the many notification obligations under the different instruments. These national sheets should make it easier to manage and to find the necessary information.

The manual incorporates these national fact sheets as well as the essential practical information on Council Framework Decision 2006/960/JHA ('Swedish Framework Decision' - SFD) and replaces the former SFD guidelines (9512/10 CRIMORG 90 ENFOPOL 125 ENFOCUSTOM 36 COMIX 346).

3. Content of the manual

The manual is divided into three parts, which are drafted so as to be consulted separately from each other, depending on the reader's intention.

The first part of the manual consists of **checklists** providing a pragmatic overview of options for information exchange and related practical aspects. These checklists help guide the user towards the appropriate contact point for the exchange of information based on lists of available systems and methods within the following key operational contexts:

– prevention and investigation of criminal offences (and illegal immigration)

– combating terrorism

– maintaining public order and security

Secondly, a **general** description presents both the national bodies involved in information exchange and the instruments for information exchange. The manual makes reference to the central role of Council Framework Decision 2006/960/JHA ('Swedish Framework Decision') and Council Decision 2008/615/JHA ('Prüm Decision') within the wider sphere of EU information exchange. However, the handbook is not limited to these instruments.

4. Way forward

The drafting of the proposed manual was included as an action point in the 3rd Action List of the Information Management Strategy and the first version of the manual was drawn up during the Irish, Cypriot, Greek, Italian and Latvian Presidencies.

With a view to further facilitating the use of the Manual on Law Enforcement Information Exchange[2], delegations are invited to disseminate the current and updated version in the light of their needs.

---

[2] Under the Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, EU law on law enforcement information exchange applies to and in the United Kingdom until the end of the transition period. After the end of the transition period, only limited acts of Union law will continue to apply to ongoing exchange of information under the conditions set out in the Agreement.

Council of the European Union
General Secretariat
Directorate-General Justice and Home Affairs
Directorate Home Affairs

Manual for Law Enforcement Information Exchange

Contents

INTRODUCTION

Purpose of this Manual

Cross-border police cooperation within the European Union relies heavily on information exchange. This manual aims at facilitating day-to-day cooperation in this respect. Its main target audience is the national SPOC, the Single Point of Contact responsible for managing the information flow between the different units and designated contact points both at national and international level.

The law enforcement[3] co-operation landscape in Europe is characterised by an increase in and speeding up of information exchange. On the one hand, it is supported by constantly developing information and communication technologies. On the other hand, there is a plethora of databases available, both national and international.

This manual aims to meet the need to find the appropriate contact or database in a specific operational context. It briefly sets out the relevant legislation without, however, losing sight of its main purpose: to facilitate cross-border information exchange.

Structure of the manual

The manual is divided into:

PART I - 'Operational Context' **-** contains a series of tables or 'checklists' that match the information contained in *PART II* and *PART III* with either the relevant legal basis or the contact point information. These checklists are divided into three main thematic areas:

- **preventing and combating crime (and illegal immigration) - Checklist A**
- **fighting terrorist offences - Checklist B**
- **maintaining public order - Checklist C**

[3] For the purposes of this manual, 'law enforcement' means the prevention, detection or investigation of terrorist offences, as defined in Directive (EU) 2017/541, or serious criminal offences, as defined in Art. 2(2) of Framework Decision 2002/584/JHA on the European Arrest Warrant (EAW).

The purpose of these checklists is to guide the reader from the point chosen as a suitable channel or method of communication in a specific operational context to the source of contact information or any appropriate legislation, rules and regulations and best practice manuals.

PART II - 'General Information' - sets out the law enforcement landscape with regard to the various communication methods and channels available to EU police forces. This second part is further broken down into three areas which cover:

- **Communication Channels (i.e. bodies involved in the exchange of law enforcement information)**
- **Information Systems and Databases used in cross-border data exchange**
- **Legislation - the legislative context and rules and guidelines relating to the main communication methods and systems**

Part III - 'National Fact Sheets' - in addendum to this note, contains national fact sheets with detailed information on contact points relevant for all aspects of cross-border exchange of information referenced throughout the document. It is the responsibility of the Member States to notify the General Secretariat of the Council promptly of any changes. By regularly updating the national fact sheets in the addendum to the manual, Member States will have complied with the many notification obligations under the different instruments. This should make it easier to manage and find this information in the future.

PART I - OPERATIONAL CONTEXT

CHECKLIST A: INFORMATION EXCHANGE FOR THE PURPOSE OF PREVENTION & INVESTIGATION OF CRIMINAL OFFENCES

Information system	**National access point**	**Legal basis**	**Handbook**
Schengen Information System / SIS II	SIRENE (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry Bureau)	The Schengen acquis as referred to in Article 1(2) of Council Decision 1999/435/EC of 20 May 1999 OJ L 239/1, 22.9.2000 Regulation (EC) 1987/2006 OJ L 381/4, 28.12.2006 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312/56, 7.12.2018	Revised version of the updated Catalogue of recommendations for the correct application of the Schengen acquis and best practices, 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Commission Implementing Decision (EU) 2017/1528 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II), OJ L 231, 7.9.2017, p. 6.

Europol / Europol Information System - EIS Index system Analysis Work Files - AWF	ENU	Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114 (applicable as from 1 May 2017)	
Interpol / I-24/7	NCB (National Central Bureau)	INTERPOL's Rules on the Processing of Data [III/IRPD/GA/2011(2014)] Rules on the Control of Information and Access to INTERPOL's Files [II.E/RCIA/GA/2004(2009)]	
DNA / PRÜM automated searching of designated national databases	National Contact Point 1st step: automated searching	Council Decision 2008/615/JHA, Articles 3 and 4 OJ L 210/1, 6.8.2008	
	2nd step: supply of further personal data and other information	National legislation Council Framework Decision 2006/960/JHA (SFD) OJ L 386/89, 29.12.2006, Corrigendum OJ L 75/26, 15.3.2007	

Fingerprints / PRÜM automated searching of national AFIS	National Contact Point 1st step: automated searching	Council Decision 2008/615/JHA, Article 9 OJ L 210/1, 6.8.2008	
	2nd step: supply of further personal data and other information	National legislation Council Framework Decision 2006/960/JHA (SFD)	
Vehicle Registration Data / PRÜM automated searching of VRD databases	National Contact Point for incoming requests	Council Decision 2008/615/JHA, Article 12, OJ L 210/1, 6.8.2008,	
	for outgoing requests	as above	
Passenger Name Record (PNR) data	Passenger Information Unit (PIU)	Directive (EU) of the European Parliament and the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime OJ L 119/132, 4.5.2016	

Visa Information System / VIS	National Central Access points	Council Decision 2004/512/EC OJ L 213/5, 15.6.2004 Council Decision 2008/633/JHA OJ L 218/126, 13.8.2008 Regulation (EC) No 767/2008 *OJ L 218, 13.8.2008* List of competent authorities the duly authorised staff of which shall have access to enter, amend, delete or consult the Visa Information System (VIS) (2016/C 187/04), OJ C 187/4, 26.5.2016	

Eurodac	National competent authorities	Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) OJ L 180/1, 29.06.2013 Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person OJ L 180/31, 29.6.2013	

CIS - Customs Information System	National access points	Council Decision 2009/917/JHA on the use of information technology for customs purposes OJ L 323/20, 10.12.2009	
European Criminal Records Information System / ECRIS	National Central Authority	Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA OJ L 151/143, 7.6.2019	ECRIS - Non-binding Manual for Practitioners available in e-format at CIRCABC https://circabc.europa.eu
Camden Assets Recovery Inter-Agency Network (CARIN)	Asset Recovery Office (ARO)	Council Decision (2007/845/JHA) of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to crime OJ L 332/103, 18.12.2007	Manual of Best Practices in the fight against financial crime: A collection of good examples of well-developed systems in the Member States to fight financial crime 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37

FIU.NET	Financial Intelligence Units (FIU)	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 658/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC OJ L 141/73, 5.6.2015 FIUs also newly regulated in Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA OJ L 186, 11.7.2019, p. 122–137	Manual of Best Practices in the fight against financial crime: A collection of good examples of well-developed systems in the Member States to fight financial crime 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37

National Firearms Focal Point network.	NATIONAL FIREARMS FOCAL POINTs (NFFP)	Communication from the Commission to the European Parliament and the Council COM(2015) 624 final. Implementing the European Agenda on Security: EU action plan against illicit trafficking in and use of firearms and explosives. 14971/15 COSI 184 ENFOPOL 404 ENFOCUSTOM 142 CYBER 125 CRIMORG 129 Joint Communication to the European Parliament and the Council. JOIN (2018) 17 final. Elements towards an EU Strategy against illicit Firearms, Small Arms & Light Weapons and their Ammunition "Securing Arms, Protecting Citizens" 11271/18 CF SP/PESC 735 CONOP 70 CODUN 26 COARM 218 Council Conclusions on the Adoption of an EU Strategy Against Illicit Firearms, Small Arms & Light Weapons & Their Ammunition. 13581/18 CONOP 98 CODUN 36 COARM 289 CF SP/PESC 985 COSI 288 ENFOPOL 565	Networks and Expert Groups related to LEWP-EFE. "Best practice Guidance for the Creation of National Firearms Focal Points" 8586/18 ENFOPOL 207

		Commission Implementing Directive (EU) 2019/69 of 16 January 2019 laying down technical specifications for alarm and signal weapons under Council Directive 91/477/EEC on control of the acquisition and possession of weapons OJ L 15, 17.1.2019, p. 22–26, article 3 Commission Delegated Regulation (EU) 2019/686 of 16 January 2019 laying down the detailed arrangements under Council Directive 91/477/EEC for the systematic exchange, by electronic means, of information relating to the transfer of firearms within the Union OJ L 116, 3.5.2019, p. 1–4, article 3	

CHECKLIST B: INFORMATION EXCHANGE FOR THE PURPOSE OF COMBATING TERRORIST OFFENCES

Information system	**National Access point**	**Legal basis**	**Handbook**
Schengen Information System / SIS II	SIRENE (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry Bureau)	The Schengen acquis as referred to in Article 1(2) of Council Decision 1999/435/EC of 20 May 1999 OJ L 239/1, 22.9.2000 Regulation (EC) 1987/2006 OJ L 381/4, 28.12.2006 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312/56, 7.12.2018	Revised version of the updated Catalogue of recommendations for the correct application of the Schengen acquis and best practices, 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Commission Implementing Decision (EU) 2015/219 of 29 January 2015 replacing the Annex to Implementing Decision 2013/115/EU on the Sirene Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2015) 326)

Europol / Europol Information System - EIS Index system Analysis Work Files - AWF	ENU	Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114 (applicable as from 1 May 2017)	
Interpol / I-24/7	NCB (National Central Bureau)	Interpol's Rules on the Processing of Data [III/IRPD/GA/2011(2014)] Rules on the Control of Information and Access to Interpol's Files [II.E/RCIA/GA/2004(2009)]	
DNA / PRÜM automated searching of designated national databases	National Contact Point 1st step: automated searching	Council Decision 2008/615/JHA, Articles 3 and 4 OJ L 210/1, 6.8.2008	
	2nd step: supply of further personal data and other information	National legislation Council Framework Decision 2006/960/JHA (SFD) OJ L 386/89, 29.12.2006, Corrigendum OJ L 75/26, 15.3.2007	

Fingerprints / PRÜM automated searching of national AFIS	National Contact Point 1st step: automated searching	Council Decision 2008/615/JHA, Article 9 OJ L 210/1, 6.8.2008	
	2nd step: supply of further personal data and other information	National legislation Council Framework Decision 2006/960/JHA (SFD)	
Vehicle Registration Data / PRÜM automated searching of VRD databases	National Contact Point for incoming requests	Council Decision 2008/615/JHA, Article 12, OJ L 210/1, 6.8.2008	
	for outgoing requests	as above	
DNA / PRÜM automated searching of designated national databases	National Contact Point 1st step: automated searching	Council Decision 2008/615/JHA, Articles 3 and 4 OJ L 210/1, 6.8.2008	*Implementation Guide - DNA Data Exchange* 7148/15 DAPIX 40 CRIMORG 25 ENFOPOL 61
PRÜM network for the supply of personal data and specified information for the prevention of terrorist offences	Prüm National Contact Point for counter-terrorism	Council Decision 2008/615/JHA, Article 16 OJ L 210/1, 6.8.2008	

Passenger Name Record (PNR) data	Passenger Information Unit (PIU)	Directive (EU) of the European Parliament and the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime OJ L 119/132, 4.5.2016	
Visa Information System / VIS	National Central Access points	Council Decision 2004/512/EC OJ L 213/5, 15.6.2004 Council Decision 2008/633/JHA OJ L 218/126, 13.8.2008 Regulation (EC) No 767/2008 OJ L 218, 13.8.2008 List of competent authorities the duly authorised staff of which shall have access to enter, amend, delete or consult the Visa Information System (VIS) (2016/C 187/04), OJ C 187/4, 26.5.2016	

Eurodac	National competent authorities	Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) OJ L 180/1, 29.06.2013 Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person OJ L 180/31, 29.6.2013	

European Criminal Records Information System / ECRIS	National Central Authority	Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA OJ L 151/143, 7.6.2019	ECRIS - Non-binding Manual for Practitioners available in e-format at CIRCABC https://circabc.europa.eu

European Criminal Records System on Third-Country National and Stateless Persons (ECRIS-TCN)	National Central Authority	Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member Stats holding conviction information on third-country nationals and stateless persons (ECIS-TCN) to supplement the European Criminal Records System and amending Regulation (EU) 2018/1726 OJ L 135/1, 22.5.2019 Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA OJ L 151/143, 7.6.2019	
Camden Assets Recovery Inter-Agency Network (CARIN)	Asset Recovery Office (ARO)	Council Decision (2007/845/JHA) of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to crime OJ L 332/103, 18.12.2007	

FIU.NET	Financial Intelligence Units (FIU)	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 658/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC OJ L 141/73, 5.6.2015 FIUs also newly regulated in Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA OJ L 186, 11.7.2019, p. 122–137	

National Firearms Focal Point network.	NATIONAL FIREARMS FOCAL POINTs (NFFP)	Communication from the Commission to the European Parliament and the Council COM(2015) 624 final. Implementing the European Agenda on Security: EU action plan against illicit trafficking in and use of firearms and explosives. 14971/15 Joint Communication to the European Parliament and the Council. JOIN (2018) 17 final. Elements towards an EU Strategy against illicit Firearms, Small Arms & Light Weapons and their Ammunition "Securing Arms, Protecting Citizens" 11271/18 Council Conclusions on the Adoption of an EU Strategy Against Illicit Firearms, Small Arms & Light Weapons & Their Ammunition. 13581/18 Commission Implementing Directive (EU) 2019/69 of 16 January 2019 laying down technical specifications for alarm and signal weapons under Council Directive 91/477/EEC on control of the acquisition and possession of weapons OJ L 15/22, 17.1.2019, article 3	Networks and Expert Groups related to LEWP-EFE. "Best practice Guidance for the Creation of National Firearms Focal Points" 8586/18 ENFOPOL 207

		Commission Delegated Regulation (EU) 2019/686 of 16 January 2019 laying down the detailed arrangements under Council Directive 91/477/EEC for the systematic exchange, by electronic means, of information relating to the transfer of firearms within the Union, OJ L 116/1, 3.5.2019, article 3	

CHECKLIST C: INFORMATION EXCHANGE FOR THE PURPOSE OF MAINTAINING PUBLIC ORDER AND SECURITY

Information system	**National Access Point**	**Legal basis**	
Network of permanent contact points concerning public order	National Contact Points	Joint Action (97/339/JHA) of 26 May 1997 adopted by the Council on the basis of Article K.3 of the Treaty on European Union with regard to cooperation on law and order and security, Article 3(b) OJ L 147/1, 05.06.1997	
PRÜM network for the supply of non-personal and personal data for the prevention of criminal offences and in maintaining public order and security for major events with a cross-border dimension	Prüm National Contact Point / Major events	Council Decision 2008/615/JHA, Article 15 OJ L 210/1, 6.8.2008 National legislation	

National Football Info Points network	National Football Info Points / NFIP	Council Decision (2002/348/JHA) of 25 April 2002 concerning security in connection with football matches with an international dimension OJ L 121/1, 8.5.2002 Council Decision (2007/412/JHA) of 12 June 2007 amending Decision 2002/348/JHA concerning security in connection with football matches with an international dimension OJ L 155/76, 15.6.2007	Council Recommendation (2007/C 314/07) of 6 December 2007 concerning a Handbook for police and security authorities concerning cooperation at major events with an international dimension OJ C 314/4, 22.12.2007 Council Resolution of 3 June 2010 concerning an updated handbook with recommendations for international police cooperation and measures to prevent and control violence and disturbances in connection with football matches with an international dimension, in which at least one Member State is involved OJ C 165/1, 24.6.2010

National Firearms Focal Point network.	NATIONAL FIREARMS FOCAL POINTs (NFFP)	Communication from the Commission to the European Parliament and the Council COM(2015) 624 final. Implementing the European Agenda on Security: EU action plan against illicit trafficking in and use of firearms and explosives. 14971/15 Joint Communication to the European Parliament and the Council. JOIN (2018) 17 final. Elements towards an EU Strategy against illicit Firearms, Small Arms & Light Weapons and their Ammunition "Securing Arms, Protecting Citizens" 11271/18 Council Conclusions on the Adoption of an EU Strategy Against Illicit Firearms, Small Arms & Light Weapons & Their Ammunition. 13581/18 Commission Implementing Directive (EU) 2019/69 of 16 January 2019 laying down technical specifications for alarm and signal weapons under Council Directive 91/477/EEC on control of the acquisition and possession of weapons, OJ L 15/22, 17.1.2019, article 3	Networks and Expert Groups related to LEWP-EFE. "Best practice Guidance for the Creation of National Firearms Focal Points" 8586/18 ENFOPOL 207

		Commission Delegated Regulation (EU) 2019/686 of 16 January 2019 laying down the detailed arrangements under Council Directive 91/477/EEC for the systematic exchange, by electronic means, of information relating to the transfer of firearms within the Union, OJ L 116/1, 3.5.2019, article 3	
Network for the protection of public figures	National access points	Council Decision 2009/796/JHA of 4 June 2009 amending Decision 2002/956/JHA setting up a European Network for the Protection of Public Figures OJ L 283/62, 30.10.2009	Manual of the European Network for the Protection of Public Figures 10478/13 ENFOPOL 173
Police and Customs Cooperation Centres	PCCC	Bilateral agreements	

PART II - GENERAL INFORMATION

1. CHANNELS OF CONTACT[4]

1.1. SPOC - Single Point of Contact

Numerous National Contact Points

Member States, as a requested as well as a requesting State, are coping with the increasing cross-border information flow by improving the efficiency of operational structures and networks - at both the national and European level. Many of the EU legal instruments on cross-border law enforcement cooperation call for the establishment of specific competent authorities / bodies / bureaux or national contact points (NCP). Police, customs or other competent authorities authorised by national law must exchange information with each other through these designated National Contact Points (NCPs) which, within a given Member State, can be in different departments of the police force or even different ministries. In order to provide an overview, lists of specific national contact points for information exchange at EU level in the area of law enforcement related data exchange are set out in Part III of this document and are regularly issued and updated by the GSC.

Single Point of Contact (SPOC)

Each Member State shall establish or designate a Single Point of Contact. The Single Point of Contact shall be the central entity responsible for coordinating and facilitating the exchange of information under the IED.

Member States shall ensure that their Single Point of Contact is equipped and empowered to carry out the tasks according to Art. 14 of IED.

[4] National bodies involved in the exchange of law enforcement information.

Typical Structure of a National SPOC (Single Point of Contact) office

The Central Unit for Police Operational Cooperation,

Platform for information exchange

*The S.C.C.O.Pol is an **inter-ministerial** structure, composed of 67 policemen, gendarmes and customs officers. The magistrates of the Office of International Cooperation on Criminal Matters (B.E.P.I.) of the Ministry of Justice also operate, in the same premises, a basic service to validate French requests for the issue of European arrest warrants and registration in the national wanted persons file of requests for arrest and foreign red notices.*

*To ensure the necessary **transversal nature** of the three channels of cooperation, a central contact point (C.C.P.) was designated at the S.C.C.O.Pol in August 2004. His/her main function is to assist the French law enforcement services in choosing the best police cooperation tool depending on the nature and complexity of the ongoing investigation. He/she checks the legality of the request, performs the first cross-checks and redirects it towards the most appropriate channel of cooperation considering the investigators' request. Only requests in relation to a Schengen alert are within the exclusive competence of the S.I.R.E.N.E. France.*

*As the result of a successful pooling of resources, the S.C.C.O.Pol handles, on a **24-hour basis**, nearly **350 000 messages per year**, on a **single secure platform**, with limited staff.*

The multi-channel jurisdiction of the S.C.C.O.Pol allows it to ensure French representation within European groups (SIS / VIS, SIS / SIRENE, heads of ENU) or Interpol groups (meeting of Interpol contact officers, notices group), and to bring a relevant operational point of view to the DRI unit responsible in France for monitoring the governance bodies of Interpol and Europol.

1.2. SIRENE bureaux

The SIRENE bureaux are crucial for SIS operations and information exchange. In each Member State, permanent SIRENE (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry) Bureaux are established as part of the Schengen *acqui* as the designated authority with central responsibility for the national section of the Schengen Information System (SIS II). They are the point of contact for SIRENE bureaux of other contracting parties and the liaison with national authorities and agencies. SIS II is a hit/no hit system based upon searches. On a 24/7 basis, the bureaux exchange data in relation to SIS II alerts, an alert being a set of data enabling authorities to identify persons or objects with a view to taking appropriate action.

1.3. EUROPOL National Unit (ENU)

Each Member State has a designated Europol National Unit (ENU) which is the liaison body between Europol and the competent national authorities. The ENUs' seconded liaison officers (LO) to Europol should ensure a live 24/7 link between the Europol headquarters in The Hague and the ENUs in the 28 Member States. Europol also hosts LOs from 10 non-EU countries and organisations. The network is supported by secure communication channels provided by Europol.

Europol[5] supports the law enforcement authorities of the Member States in preventing and combating organised crime, serious international crime and terrorism involving two or more Member States. In order to collect, store, process and analyse personal data and exchange information and intelligence, Europol is dependent on data input from Member States. The Europol Regulation lays down the different information tasks and the rules on the use of data and exchange of data with third parties on the basis of a robust data protection and security regime.

[5] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114 (applicable as from 1 May 2017)

1.4. INTERPOL National Central Bureaux (NCB)

The **National Central Bureaux (NCB)** at the national police headquarters play a central role concerning the processing of data in the Interpol Information System provided by their countries. They are entitled to directly access the system, which includes:

- the recording, updating and deletion of data directly in the organisation's police databases as well as the creation of links between data;
- direct consultation of these databases;
- the use of Interpol's notices and circulars for the transmission of requests for cooperation and international alerts.

NCBs can rapidly search and cross-check data with 24/7 direct access to databases containing information on suspected terrorists, wanted persons, fingerprints, DNA profiles, lost or stolen travel documents, stolen motor vehicles, stolen works of art, etc.

As far as possible, NCBs should allow the criminal investigation authorities of their countries involved in international police cooperation to have access to the Interpol Information System. NCBs control the level of access which other authorised users of their countries have to Interpol services and can request to be informed of enquiries made to their national databases by other countries.

1.5. Prüm National Contact Points

The 'Prüm Decisions'[6] opened up a new cross-border dimension of crime fighting by providing for mutual cross-border online access to designated national DNA databases, automated fingerprint identification systems (AFIS) and vehicle registration databases (VRD). In order to supply data, a specific National Contact Point (NCP) is designated for each type of data exchange in each participating Member State[7]. Data protection and tailor-made data security provisions take particular account of the specific nature of online access to these databases. The supply of personal data requires an adequate level of data protection and security, mutually tested and agreed upon by the Member States before launching data exchange.

1.5.1. Prüm NCP – DNA and Fingerprints

In the case of DNA and fingerprint data, the automated comparison of biometric reference data is based on a hit/no hit system. Reference data do not allow the data subject to be immediately identified. In the event of a hit, the NCP of the searching Member State may therefore request additional specific personal data. The supply of such supplementary data has to be requested through mutual assistance procedures, including those adopted pursuant to the 'Swedish Framework Decision', and is governed by the national law, including the legal assistance rules, of the requested Member State.

---

6 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210/1, 6.8.2008; Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime**,** OJ L 210/12, 6.8.2008.

7 5010/15 JAI 1 DAPIX 1 ENFOPOL 1 CRIMORG 1.

1.5.1.1. Best Practice Guidelines for fingerprint searches

When utilising the Prüm automated fingerprints search facility, a requesting Member State should follow the recommendations set out in the document *Good Practices for consulting Member States' databases* (14885/1/08 REV 1). It acknowledges the limited search capacities of **dactyloscopic databases** and recommends that the following practices be promoted at operational level:

- Whether or not to consult Member States' fingerprint databases, and the order in which such searches are carried out and repeated, are investigative decisions taken on a case-by-case basis and should not be systematically predetermined.

- Other Member States' fingerprint databases should in principle not be searched until the requesting State's own fingerprint database(s) have been searched.

- Whether to search one or more Member States' databases should take account especially of:

  – the seriousness of the case;

  – and/or existing lines of investigation, in particular information pointing in the direction of a Member State or group of Member States;

  – and/or the specific requirements of the investigation.

- General searches should only be undertaken where the good practice in points 1 to 3 has been exhausted.

Examples of automated data exchange under the Prüm Council Decisions

In 2011, genetic material was entered in the Czech national DNA database during the investigation of a murder. The investigation was being conducted against a suspect who had fled abroad. The genetic material was obtained from a cigarette butt in an ashtray in the apartment where the crime was committed. By searching the Austrian DNA database in 2014, it was found that the same profile had been processed in Austria. Further personal data was exchanged by the SPOCs of both countries via police cooperation. Afterwards, the criminal justice department in Austria was contacted and asked to surrender the suspect for criminal prosecution to the Czech Republic via legal assistance in criminal matters.

In 2005, a DNA profile was entered in the Czech national DNA database during the investigation of a robbery. A suspect was identified in 2014 after searching the Austrian DNA database. The Austrian side was asked to supply a current photograph and other personal data via the SPOCs.

1.5.2. Prüm NCP - Vehicle Registration Data (VRD)

With regard to VRD, searches may be conducted with a full chassis number in one or all participating Member States, or with a full registration number in one specific Member State. Information will be exchanged by NCPs designated both for incoming and outgoing requests. Member States give each other online access to national VRD for

(a) data relating to owners or operators, and

(b) data relating to vehicles.

Member States use a version of the European Vehicle and Driving Licence Information System (EUCARIS) software application especially designed for Prüm purposes to conduct such searches. VRD searches differ from DNA and fingerprint searches in that they return both personal and reference data in the event of a hit. As with other automated searches it is understood that the supply of personal data is subject to the appropriate level of data protection being applied by the receiving Member States.

1.5.3. Prüm NCP for the prevention of terrorism

On request or on their own initiative, designated NCPs may exchange information on persons suspected of committing terrorist offences. The data shall comprise the surname, first names, date and place of birth of the suspect and a description of the circumstances giving rise to the belief that the data subject will commit criminal offences linked to terrorist activities.

The supplying Member State may, in compliance with national law, impose conditions on the use made of such data and information by the receiving Member State, which is bound by any such conditions.

1.5.4. Prüm NCP for major events

Member States hosting major events with an international dimension have to ensure the security of the event both from a public order perspective and a counter-terrorism perspective. Depending on the nature of the event (political, sporting, social, cultural or other), one perspective may be more relevant than the other. However, both aspects need to be considered although possibly dealt with by different authorities. Special attention is directed at the phenomenon of travelling violent offenders (TVO), in particular with regard to international football matches.

For the purposes of preventing criminal offences and maintaining public order and security in connection with major events and similar mass gatherings (of a political, sporting, social, cultural or other nature), disasters and serious accidents with a cross-border impact, designated NCPs supply each other, on request or on their own initiative, with

- non-personal data, or
- personal data, if any final convictions or other circumstances give reason to believe that the data subjects will commit criminal offences at the events or pose a threat to public order and security.

Personal data may be processed only for the above-mentioned purposes and for the specified events for which they were supplied. The data supplied must be deleted without delay once these purposes have been achieved, in any case after not more than one year. Information is supplied in compliance with the supplying Member State's national law.

1.5.4.1. Handbook for cooperation on major events with an international dimension[8]

This handbook contains guidelines and suggestions for law enforcement authorities tasked with ensuring public security at major events such as the Olympic Games or other major sporting events, social events or high-level political meetings.

The Handbook, which is constantly amended and adjusted in accordance with the development of best practices, contains guidance on information management and event management as well as on event-related and strategic evaluation. Annexed standard forms concern:

- requests for liaison officers;
- risk analysis on potential demonstrators and other groupings;
- exchange of information regarding individuals or groups posing a terrorist threat;
- a list of reference documents;
- a table containing permanent national contact points concerning public order.

1.6. National (Police) Football Information Point (NFIP)[9]

Further to the Prüm NCP for major events and with particular regard to international football matches, a National Football Information Point (NFIP) in each Member State is tasked with exchanging relevant information and developing cross-border police cooperation. Tactical, strategic and operational information can be used by the NFIP itself or is forwarded to the relevant authorities or police services.

Contacts between the police services of the different countries involved in an event are coordinated and, if necessary, organised by the NFIP. The CIV-based website for NFIPs (www.nfip.eu) disseminates information and advice on available legal and other options concerning safety and security in connection with football matches.

---

8 Council Recommendation 2007/C 314/02 of 6 December 2007 concerning a Handbook for police and security authorities concerning cooperation at major events with an international dimension, OJ C 314/4, 22.12.2007).

9 Council Decision 2002/348/JHA of 25 April 2002 concerning security in connection with football matches with an international dimension, OJ L 121/1 8.5.2002.

The NFIP coordinates the processing of information on high-risk supporters with a view to preparing and taking the appropriate measures to maintain law and order when a football event takes place. Such information includes, in particular, details of individuals actually or potentially posing a threat to law and order and security. Information should be exchanged on the forms[10] contained in the appendix to the Football Handbook.

1.6.1. The Football Handbook[11]

The Football Handbook is annexed to Council Resolution 2006/C 322/01 and provides examples of how the police should cooperate at international level in order to prevent and control violence and disturbances in connection with football matches. The content consists in particular of recommendations concerning:

- information management by police forces;
- the organisation of cooperation between police forces;
- a checklist for media policy and communication strategy (police/authorities).

1.7. National Firearms Focal Points (NFFP)

Further to the EU Action Plan of 2 December 2015 COM (2015) 624 final, under "Building a better intelligence picture", the Commission invited all Member States to set up inter-connected national focal points on firearms to develop expertise and improve analysis and strategic reporting on illicit trafficking in firearms notably through the combined use of both ballistic and criminal intelligence.

---

10 Council Decision 2007/412/JHA of 12 June 2007 amending Decision 2002/348/JHA concerning security in connection with football matches with an international dimension, OJ L 155/76, 15.6.2007.

11 Council Resolution concerning an updated handbook with recommendations for international police cooperation and measures to prevent and control violence and disturbances in connection with football matches with an international dimension, in which at least one Member State is involved ('EU Football Handbook') (2016/C 444/01)OJ C 444, 29.11.2016, p. 1–36.

The EU Strategy against illicit Firearms, Small Arms & Light Weapons and their Ammunition "Securing Arms, Protecting Citizens",[12] under 'Compliance through monitoring and enforcement - operational cooperation-' stated that 'the EU will improve cross-border cooperation between judicial and law-enforcement authorities, encourage the relevant Member State authorities, including customs authorities, to establish national focal points on firearms, produce better analysis of all information available in the area of illicit firearms and ensure full participation in the exchange of information with Europol in the area of firearms trafficking.' This was endorsed by the Council, turning it into a fully-fledged EU Strategy.[13]

The NFFP gathers, analyses and improves the information flow regarding the criminal use and the illicit trafficking of firearms into and within the Member States and across into the EU at a strategic and operational level by means of a co-ordinated collection and sharing of information to enhance the intelligence picture and to better inform law enforcement agencies. Information should be exchanged following the guidelines contained within the EFE & EMPACT Firearms Best Practice Guidance.

1.7.1. NFFP Best Practice Guidance

The Best Practice Guidance[14] for the creation of NFFPs provides examples on how the NFFP should carry out the following tasks:

- Establishing a Repository for firearms related intelligence both criminal and ballistic,
- Establishing a Repository for all lost, stolen and recovered firearms,
- Tracing of all seized firearms from manufacturer to the last legal owner,
- Analysing of firearms tracing data to identify firearms type, make, model, calibre and country of manufacture,
- Providing data, statistics, information, assessments and reports for use within MS,

12 JOIN(2018) 17 final, 1.06.2018.
13 Council conclusions of 19 November 2018 – Document 13581/18.
14 8586/18

- Functioning as a technical point of contact with UNODC,
- Fulfilling the requirements of the United Nations Illicit Flows Questionnaire (UN-IAQF),
- Promoting international cooperation.

By having access to the relevant databases including the Europol Information System (EIS), Schengen Information System (SIS2) and iARMS and following the Best Practice Guidance, the NFFP would be able to undertake and provide the exchange of information, undertake internal and incoming research requests, assist and co-ordinate operational actions whilst maintaining sufficient control of intelligence, data and information on a national level which will allow for the prompt and regular dissemination of that data to Europol and other law enforcement institutions and agencies such as UNODC.

1.8. Police and Customs Cooperation Centres (PCCC)

PCCCs are established on the basis of bi- or multilateral agreements in accordance with Article 39(4) of the Convention implementing the Schengen Agreement (CISA). In these agreements, the contracting parties define the basis for their cross-border cooperation, including the tasks, legal framework, and procedures for establishing and operating the centres. PCCCs bring together staff from neighbouring countries and are closely linked to national bodies dealing with international cooperation (NCPs, Interpol NCB, ENU, SIRENE Bureaux).

PCCCs provide advice and non-operational support to the national operational police, customs and other agencies in the border region where they are located. PCCC staff are tasked to rapidly provide information requested

At the end of 2016, 8 of the 59 existing PCCCs were linked to SIENA, Europol's secure information exchange network application. Information exchange via PCCCs relates mainly to petty and moderately serious crime, illegal migration flows and public order problems. Such information may include identification of drivers or verification of the appropriateness and authenticity of ID and travel documents.

The contracting parties may jointly decide to transform a PCCC into a regional operational coordination centre at the service of all the agencies concerned, in particular in the case of regional incidents (natural catastrophes) or major events (Olympic Games, Football World Cup, etc.).

If a PCCC receives information within the national central unit's remit, that information must be forwarded immediately to the SPOC/central unit. Should a PCCC receive information of obvious interest for Europol, it may forward this information to the ENU located within the SPOC which will relay it to Europol itself.

Example of Information exchange through a PCCC

EPICC ('Euregio Police Information and Cooperation Centre') is the short name of PCCC Heerlen.

It was created ad hoc (no specific legal instrument) in 2005 at the initiative of 'NeBeDeAgPol', an association of police chiefs in the Euregio Meuse-Rhine, situated in the border region between the Netherlands, Belgium, and Germany - one of the most densely populated border areas in the European Union.

In this PCCC, around thirty Belgian, German and Dutch police officers work together on one platform.

These agents have on-site access to most of the content of their respective country's databases. This enables them to provide - within a very short time - accurate, complete and reliable answers to police requests for information concerning BE, DE or NL. The information exchange between the three delegations of EPICC is made via the Europol application 'SIENA'.

EPICC collects and analyses available police information in the border region in order to detect, describe and follow border security problems (new phenomena or modi operandi, groups of criminals acting in the border region, events or persons requiring particular attention, etc.).

Thanks to its special expertise and mixed composition, PCCC Heerlen can provide efficient support during the preparation and execution of cross-border operations, investigations or surveillance measures.

1.9. Liaison Officers

According to Article 47 of the Convention implementing the Schengen Agreement (CISA), Member States *'may conclude bilateral agreements providing for the secondment, for a specified or unspecified period, of liaison officers from one [Member] State to the police authorities of another [Member] State'*. The role of liaison officers is to establish and maintain direct contacts to further and accelerate cooperation for the purpose of combating crime, particularly by providing assistance. Liaison officers are not empowered to execute any police measures autonomously. They guarantee fast and effective cooperation, based on personal contact and mutual trust, by:

- facilitating and expediting the collection and exchange of information;
- executing requests for mutual police and judicial assistance in criminal matters;
- organising and ensuring cross-border operations.

Liaison officers may be posted to other Member States, third countries or EU agencies or international organisations. The Compendium[15] on law enforcement liaison officers, updated annually by the General Secretariat of the Council, explains the work and tasks of the liaison officers and contains lists of liaison officers including contact details.

Based on past and on-going experiences in different host countries and with a view to achieving greater pooling of Member States' activities vis-à vis third countries in terms of both the work of the liaison officers and technical cooperation, some good practices have been identified, which are set out in the Compendium. It is suggested that the Member States' liaison officers and their relevant authorities apply these whenever appropriate.

[15] 'Update of the Compendium on law enforcement liaison officers (2018)', 10095/1/18 REV 1 ENFOPOL 397 JAIEX 84 COMIX 422

Typical Examples of Information Exchange between Liaison Officers

- *Liaison Officers may be tasked with ensuring contact in order to establish direct cooperation in specific cases such as drug related-crimes.*
- *Liaison Officers can provide specific information on national rules and legislation regarding international police cooperation or judicial assistance in criminal matters.*
- *Liaison Officers, in some cases, maintain up-to-date lists of responsible authorities within their Member State.*
- *Liaison Officers have also been tasked in some MS with handling requests for cooperation under Article 17 of the Prüm Decision (Joint Operations). For example, the Danish LO at Europol was asked by the Czech Republic to forward a request to Denmark to assign 4 Danish police officers to assist with a case involving both MS.*

1.10. Asset Recovery Offices (ARO) of the Member States

Financial crime covers a wide array of activities such as counterfeiting, corruption and fraud (e.g. credit card fraud, mortgage, medical or securities fraud, bribery or embezzlement, money laundering, identity theft and tax evasion). Improved cooperation is achieved through closer cross-border collaboration between Asset Recovery Offices (ARO), Financial Intelligence Units (FIU) and police and customs authorities.[16]

[16] Manual of best practices in the fight against financial crime: A collection of good examples of well-developed systems in the Member States to fight financial crime, 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144.

Following the adoption of Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime[17], all Member States have since established and designated asset recovery offices (AROs). These specialised units have evolved into a close-knit network of specialists who can directly exchange information on matters pertaining to the recovery of assets via the SIENA system. Under the auspices of the EU Commission and Europol, the ARO Network facilitates cooperation between AROs of the Member States and the strategic discussion and exchange of best practices. The Europol Criminal Assets Bureau (ECAB) acts as a focal point for asset recovery within the EU.

The provisions laid down in Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union[18] will further enhance the effectiveness of cooperation between the asset recovery offices within the European Union. Member States are called upon to transpose the Directive by 4 October 2016.

The **Camden Assets Recovery Inter-Agency Network (CARIN)**, established in 2004 to support the cross-border identification, freezing, seizure and confiscation of property related to crime, enhances the mutual exchange of information regarding different national approaches extending beyond the EU.

As of 2015, the CARIN Network includes practitioners from 53 jurisdictions and 9 international organisations which serve as contact points for the purpose of rapid cross-border exchange of information, on request or spontaneously. National AROs cooperate among themselves or with other authorities facilitating the tracing and identification of proceeds of crime. While all Member States have established an ARO, major differences exist between the Member States in terms of organisational setup, resources and activities.

---

17 Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, OJ L 332/103, 18.12.2007.

18 Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, OJ L 127/39, 29.4.2014.

Information exchanged may be used according to the data protection provisions of the receiving Member States and is subject to the same data protection rules as if it had been collected in the receiving Member State. Spontaneous information exchange in line with this Decision, applying the procedures and time limits provided for in the Swedish Framework Decision, is to be promoted.

1.11. Money Laundering - Cooperation between Financial Intelligence Units (FIU)[19] [20]

Relevant information on any fact which might be an indication of money laundering or terrorist financing should be reported to the national Financial Intelligence Units (FIUs). FIUs analyse information received on a case by case basis with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing. The FIU serves as a central national unit for receiving, analysing and disseminating to the competent authorities the results of its analyses. Being operationally independent and autonomous, the FIU carries out it functions freely, including the autonomous decision to analyse, request, and disseminate specific information.

FIUs serve as well as national contact points for the cross-border exchange of information. As with Asset Recovery Agencies, they vary considerably between the Member States as to their organisational setup, functions and resources. They are placed either under judicial authorities or within police bodies or created as a 'hybrid', combining police and prosecutor competencies. This diversity may sometimes lead to obstacles in international cooperation.

---

19 Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, OJ L 186, 11.7.2019, p. 122–137.

20 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 658/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141/73, 5.6.2015.

However, taking into account the transnational nature of money laundering and terrorist financing, coordination and cooperation between FIUs are extremely important. In order to improve such coordination and cooperation, and, to ensure that suspicious transaction reports reach the FIU of the Member State where the report would be of most use, detailed rules are laid down in Directive (EU) 2015/849. With a view to providing rapidly, constructively and effectively the widest range of cross-border cooperation, Member States should, in particular, ensure that their FIUs exchange information freely, spontaneously or upon request with third-country financial intelligence units.

Improving the exchange of information between FIUs within the Union, the use of secure facilities, in particular, the decentralised FIU.NET computer network. All 28 FIUs are connected to the FIU.NET. It has developed over recent years from a secure basic tool for structured bilateral information exchange to a secure multifunctional tool for multilateral information exchange, with case management features as well as semi-automated standardisation of processes. In FIU.NET, each new feature and automated process is optional, with no strings attached. The individual FIUs can decide which of the possibilities and features offered by FIU.NET to use; they just use the features they feel comfortable with and exclude the ones they do not need or want to use.

1.12. Naples II Convention[21]

Member States assist one another in the framework of the Naples II Convention in order to prevent and detect infringements of national customs provisions and prosecute and punish infringements of Community and national customs provisions. With regard to criminal investigations, the Convention lays down procedures under which customs administrations may act jointly and exchange data, spontaneously or on request, concerning illicit trafficking activities.

Requests are submitted in writing in an official language of the Member State of the requested authority or in a language acceptable to that authority. A form sets out the standard for communication of information. The authorities concerned communicate all information which may assist in preventing, detecting and prosecuting infringements. They exchange personal data, i.e. all information relating to a natural person who is identified or identifiable.

---

21 Council Act of 18 December 1997 drawing up, on the basis of Article K.3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations, OJ C24/1, 23.01.1998.

In order to provide the assistance required, the requested authority or the competent authority which it has addressed shall proceed as though it were acting on its own account or at the request of another authority in its own Member State.

The Handbook for the Naples II Convention on mutual assistance and cooperation between customs administrations is divided in three parts, which set out:

- the general provisions in 13615/05 ENFOCUSTOM 61 + COR 1 (CZ);
- the national fact sheets, as updated in 2016, in 15429/16 JAI 1028 ENFOCUSTOM 238;
- the annexes, including the standard forms for communication of information, in 13615/05 ENFOCUSTOM 61 ADD 1.

1.13. Passenger Information Unit (PIU)

In the framework of Directive 2016/681[22], each Member State establishes or designates a passenger information unit (PIU). Such units are competent for processing passenger name record (PNR) data received from air carriers[23] and, furthermore, constitute the main channel for information exchange between Member States and with Europol. Two or more Member States may establish or designate a single authority to serve as their common PIU.

The processing of PNR data serves mainly the assessment of air passengers in order to identify persons who require further examination by national authorities competent for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The directive applies to extra-EU flights and may be applied to intra-EU flights as well if a Member State decides to do so.

---

22 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119/132, 4.5.2016.

23 The Directive does not affect the possibility of Member States to provide, under their national law, for a system of collecting and processing PNR data from non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services - including the booking of flights - for which they collect and process PNR data, or from transportation providers other than those specified in the Directive, provided that such national law complies with Union law.

The assessment of PNR data facilitates the identification of persons who were, prior to such assessment, not suspected of involvement in terrorist offences or serious crime. In line with EU data protection policy, the processing of such data should be both relevant and necessary, and proportionate to the specific security goals pursued by the directive.

The PIUs are responsible for:

- at domestic level, collecting PNR data from air carriers, storing and processing these data and transferring them, or the result of processing them, to the national competent authorities;
- at Union level, exchanging PNR data and the result of processing thereof

    a) among themselves. In cases of emergency, however, and under certain conditions, the above national competent authorities may ask the PIU of another Member State directly to provide them with PNR data kept in the latter's database; and

    b) with Europol, which is entitled, within the limits of its competences and for the performance of its tasks, to request such data from the PIUs.

PIUs shall carry out their tasks exclusively within a secure location within the territory of a Member State. PNR data provided to the PIUs must be stored in a database for a period of five years after their transfer to the PIU of the Member State of arrival or departure. However, six months after their transfer, all PNR data must be depersonalised by masking out those data elements which are set out in the directive and which could serve to identify the data subject directly. The result of processing shall be kept by the PIU only as long as necessary to inform the relevant national competent authorities and to inform the PIUs of other Member States of a positive match.

The PIU processes only those data listed in Annex I of the directive for the purposes of:

- carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State in order to identify persons who require further examination by national authorities and, where required, by Europol;

- responding, on a case-by-case basis, to a request from the competent authorities to provide and process PNR data for specific cases, and to provide these authorities and, where appropriate, Europol with the results of such processing;

- analysing PNR data for the purpose of updating or creating new criteria applied in order to identify passengers that may be involved in a terrorist offence or serious crime.

When carrying out such assessments, the PIU may either compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, and in accordance with Union, international and national rules applicable to such databases, or process PNR data against relevant predetermined criteria. These predetermined criteria must be targeted, proportionate and specific. It is up to the PIUs to establish and regularly review those criteria in cooperation with the relevant competent authorities. These criteria shall not be based on sensitive personal data such as race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

With regard to persons identified, the PIU transmits all relevant and necessary PNR data or the result of processing thereof to the corresponding PIU of the other Member States. These PIUs will transmit the information received to their own competent authorities.

The data protection officer appointed by the PIU is responsible for monitoring the processing of PNR data. A data subject is entitled to contact the data protection officer as the single point of contact on all issues relating the processing of that data subject's PNR data.

All transfers of PNR data by air carriers to the PIUs are to be made by electronic means that ensure technical security. To that effect, both the common protocols which air carriers have to comply with when transferring data, and supported data formats which ensure the readability of the data by all relevant parties, are defined at EU level.[24]

[24] Commission Implementing Decision (EU) 2017/759 of 28 April 2017 on the common protocols and data formats to be used by air carriers when transferring PNR data to Passenger Information Units, OJ L 113/48, 29.04.2017.

1.14. EES national access points

The Entry/Exit System[25] (EES) aims primarily at improving the Union's external border management and is used to that effect by border, immigration and visa authorities[26]. The system registers electronically the time and place of entry and exit of certain third-country nationals admitted for a short stay to the territory of the Member States and calculates the duration of their authorised stay. The EES is operated at external borders. Member States which apply the Schengen *acquis* in full introduce the EES at their internal borders with Member States which do not yet apply the Schengen *acquis* in full but which either do operate or do not operate the EES. No biometric functionalities are introduced by Member States which do not apply the Schengen *acquis* in full.

Further to border, immigration and visa authorities, the EES may be consulted under the conditions laid down in the Regulation by national 'designated authorities'. They consult it for law enforcement purposes, and to enable the generation of information for investigations related to terrorist offences and of other serious criminal offences, including the identification of perpetrators, suspects and victims of such offences who have crossed the external borders.

Member States designate the authorities entitled to consult the EES for law enforcement purposes. Furthermore, each Member State designates a central access point to the EES. Separate from the 'designated authorities', the central access performs its tasks fully independently of the 'designated authorities' and should not receive any instructions from them as regards the outcome of the verification, that is the process of comparing sets of data to establish the validity of a claimed identity, so to ensure that it is carried out independently. Only duly empowered staff of the central access point is authorised to access the EES.

---

25 Regulation (EU 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, OJ L 327/20, 9.12.2017.

26 The Commission will determine the date from which EES is to start operations once the conditions set out in Article 66 of Regulation (EU 2017/2226 are met.

Operating units within the 'designated authorities' are authorised to request EES data through the central access points. To that end, the operating unit has to submit a reasoned electronic or written request to a central access point for access to EES data. The central access point checks whether the conditions for access, as laid down by the Regulation, are fulfilled, and in case of a positive outcome, processes the request. The EES data will then be transmitted to an operating unit in a way that the security of data is not compromised.

The conditions to be scrutinised for access to EES data for law enforcement purposes are:

- access for consultation is necessary for the purpose of law enforcement;
- access for consultation is necessary and proportionate in a specific case;
- evidence or reasonable grounds exist to consider that the consultation of EES data will contribute to the prevention, detection or investigation of any of the criminal offence in question, in particular where there is a substantial suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence fall under a category covered by the Regulation.

Additionally, access to EES as a tool for the purpose of identifying the suspect, perpetrator or victim of such offences is allowed where

- a prior search has been conducted in national databases;
- in the case of searches with fingerprints, a prior search has been launched under Council Decision 2008/615/JHA ('Prüm Decision') where comparisons of fingerprints are technically available, and either that search has been fully carried out, or that search has not been fully carried out within two days of being launched.

A request for consultation of the VIS on the same data subject may be submitted in parallel to the request for consultation of the EES in accordance with the conditions laid down in Council Decision 2008/633/JHA.[27]

Finally, access to EES as a tool to consult the travel history or the periods of stay on the territory of the Member States of a known suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence is allowed when the above principles are met.

1.15. ETIAS National Unit[28]

The European Travel Information and Authorisation System (ETIAS) supports[29] information exchange for the purposes of border management, law enforcement and counter-terrorism. ETIAS aims to determine the eligibility of visa-exempt third-country nationals prior to their travel to the Schengen Area and arrival at external border crossing points. ETIAS provides a travel authorisation, which is by nature distinct from a visa but constitutes a condition of entry and stay, and indicates that the applicant does not pose a security, illegal immigration or high epidemic risk.

ETIAS consists of

- the ETIAS information system, including the ETIAS watchlist;
- the ETIAS Central Unit, which is part of the European Border and Coast Guard Agency;
- the ETIAS National Units.

---

27 Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of the Member States and by Europol for the purposes of prevention, detection or investigation of terrorist offences and of other serious criminal offences, OJ L 218/129, 13.8.2008.

28 Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236/1, 19.9.2018.
Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS), OJ L 236/72, 19.9.2018.

29 The Commission will determine the date from which ETIAS is to start operations once the conditions set out in Article 88 of Regulation (EU) 2018/1240 are met.

If in the automated application process a correspondence ("hit)" occurs between data in the application file and data in the ETIAS information systems, specific risk indicators or alerts in the consulted EU information systems, the ETIAS Central Unit is tasked to verify that hit and, where a correspondence is confirmed or where doubts remain, to launch the manual processing of the application in the Member State identified.

Subsequently, it is the ETIAS National Unit of the Member State concerned that processes manually the application in question. It will get access to the application file and any linked application file, as well as to any hit triggered during the automated processing. Following the manual processing, the national unit responsible will eventually issue or refuse, in line with the provisions of the Regulation, a travel authorisation. To that end, the national unit may request additional information or documentation.

A travel authorisation is to be refused if the applicant

- used a travel document which is reported as lost, stolen or misappropriated or invalidated in SIS;
- poses a security risk;
- poses an illegal immigration risk;
- poses a high epidemic risk;
- is a person for whom an alert has been entered in SIS for the purpose of refusing entry or stay;
- fails to reply to a request for additional information or documentation, or to attend an interview.

The ETIAS National Units are responsible for examining applications and deciding whether to issue or refuse, annul or revoke travel authorisations. To that end, the national units should cooperate with each other and with Europol for the purpose of assessing applications.

A national unit may decide to refuse a travel authorisation, to annul a travel authorisation, where it becomes evident that the conditions for issuing it were not met at the time when it was issued, or to revoke a travel authorisation, where it becomes evident that the conditions for issuing it are no longer met. Applicants concerned have the right to appeal. Appeals have to be conducted in the Member State that has taken the decision on refusal, annulment or revocation, and in accordance of the national law of that Member State. The competent national unit is tasked to provide applicants with information regarding the appeal procedure.

Border authorities competent for carrying out border checks at external crossing points shall consult the ETIAS Central system using the data contained in the machine readable zone of the travel document. Immigration authorities checking or verifying whether the conditions for entry or stay on the territory of the Member States are fulfilled have access to search the ETIAS Central system.

Only in specific cases and only when it is necessary for the purposes of preventing, detecting or investigating terrorist or serious criminal offences, Member States' designate law enforcement authorities are entitled to request consultation of personal data recorded in the ETIAS Central System. Directive (EU) 2016/680 ("Police Directive") applies to the processing of such personal data by the designated authorities of the Member States pursuant to the ETIAS Regulation.

1.16. Interoperability

The main objective of the 'interoperability package'[30] is to improve the Union's data management architecture for border management and security with a view to facilitating the correct identification of persons, which re not European citizens but third-country nationals. Interoperability between the EES (see pt. 3.18), VIS (see pt. 3.7), ETIAS (see pt. 3.19), Eurodac (see pt. 3.8), SIS (see pt. 3.2), and ECRIS-TCN (see pt. 3.13.2) aims at allowing these EU information systems to supplement each other. To that end, a European search portal (ESP), a shared biometric matching service (shared BSM) a common identity repository (CIR) and a multiple-identity detector (MID) are to be established.[31]

(a) To ensure the systematic use of the above EU information systems, the designated authorities entitled to have access to at least one of them, the CIR and the MID, to Europol data or to the Interpol SLTD and TDAWN database (see pt. 2.4), should use the ESP, which allows for the simultaneous querying of these information systems.

(b) The common identity repository (CIR) creates an individual file for each person that is registered in those information systems, and is understood as a shared container for identity data, travel data and biometric data of persons registered in the systems. CIR should be part of the technical architecture of the systems and serve as the shared component between them for storing and querying the identity data, travel data and biometric data they process.

---

30 Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135/27, 22.5.2019.
Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019.

31 The Commission will determine the date from which the provisions of the Regulations related to the ESP, the shared BMS, the CIR and the MID will apply.

Access to CIR is granted for purposes such as

- the correct identification of person registered in the EU information systems or, where necessary,

- to assist law enforcement authorities in the prevention, detection and investigation of terrorist offences nor serious criminal offences.

Where for a couple of different reasons a police authority is unable to identify a person, this authority can query the CIR. To this end, Member States empower, on the basis of national legislation, their competent authority to do so and establish the procedures, conditions and criteria for such checks. The query is carried out either on the basis of freshly taken fingerprints of that person, or, if that option fails, on the basis of identity data of the person in combination with travel document data.

Should the query indicate that data on that person are stored in the CIR, the police authority shall get the surname, first name, date of birth, place of birth, nationality, gender, previous names, if applicable, where available pseudonyms or aliases, as well as, where available, information on travel documents. Furthermore, the police may, if entitled by national legislation, carry out biometric CIR queries in the event of a natural disaster, an accident or a terrorist attack and solely for the purposes of identifying unknown persons, who are unable to identify themselves, or unidentified human remains.

Querying the CIR for law enforcement purposes, in particular where there is a suspicion that the suspect, perpetrator or victim of a terrorist offence or serious crime is a person whose data are stored in the information systems, the designated authorities and Europol may consult CIR in order to know whether data on a specific person are stored. In the affirmative, the CIR provides, following the automated verification of the presence of a match in the system (match-flag functionality), a reply in form of a reference indicating the information system, which the contains matching data. The match-flag type response should be used only for the purpose of submitting an access request to the underlying EU information system. Such a of response should not reveal personal data of the individual concerned other than an indication that data are stored in one of the systems.

No adverse decision for the individual concerned should be made by the authorised end-user solely on the basis of the occurrence of a match flag. Access by the end-user to a match-flag is therefore supposed to constitute a very limited interference with the right to protection of personal data of the individual concerned, while allowing the designated authorities to request access to personal data more effectively. Full access to data for law enforcement purposes remains subject to the conditions and procedures laid down in the Eurodac Regulation (see pt. 2.7).

(c) The multiple-identity detector (MID) creates and stores links between data in the different EU information systems. In the case of law enforcement; the MID in the CIR and in SIS shall be launched where an SIS alert on a person is created or updated, or where a data record is created or modified in ECRIS-TCN. It shall only be launched in order to compare data available in one EU information system with data available in another EU information system. Verification of different identies shall be done manually by either the respective SIRENE Bureau or the respective central authorities.

The Commission will:

- determine the date from which the provisions of the Regulations related to the ESP, the shared BMS, the CIR and the MID will apply;

- in close cooperation with the Member States, eu-LISA and other relevant Union agencies, make available a practical handbook for the implementation and management of the interoperability components. The practical handbook shall provide technical and operational guidelines, recommendations and best practices.

1.17. Choosing the channel – Commonly used criteria

In a Member State, the SPOC[32] carries out a crucial role in determining the most appropriate and relevant channel by gathering all requests (both incoming and outgoing) dealt with by the unit. In the interests of efficiency, national authorities allow investigators considerable autonomy in choosing the channel deemed most appropriate for investigation. The most commonly-used communication channels are as follows:

- SIRENE via the contact points of each Schengen State for SIS
- EUROPOL via the Europol National Units / Europol Liaison Officers (the default channel of communication to be used for all exchanges of information under the IED and the information to be provided to the Single Points of Contact in relation to the exchange of information directly between the competent law enforcement authorities)
- INTERPOL via the National Central Bureaux at the National Police Headquarters
- Liaison Officers
- Mutual Assistance channels used between customs authorities (Naples II)
- Bilateral channels based on cooperation agreements at national, regional and local level (PCCCs)

The general rules provide that a request is sent through one channel only. However, in exceptional cases, a request may be sent through different channels at the same time. In such cases this should be clearly indicated to all parties in an appropriate manner. Similarly, a change of channel must be communicated to all parties, along with the reason for the change.

In order to avoid thematic overlaps or situations where a request is unnecessarily sent more than once through different channels, the relevant desk officer (SIS, Europol, Interpol, bilateral liaison officer) in the requesting State may determine the most appropriate route for a request for information on the basis of the following criteria:

[32] SPOC Guidelines, 10492/14 DAPIX 75 ENFOPOL 157 and 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1).

- geographical criteria, i.e. nationality/residence/origin of person or object concerned is known and the request concerns the communication of details (address, phone number, fingerprints, DNA, registration, etc.)

- thematic criteria, i.e. organised crime, serious crime, terrorism; confidentiality/sensitivity; channel used for previous related request

- technical criteria; i.e. the need for secure IT channels

- urgency criteria, i.e. an immediate risk to a person's physical integrity, immediate loss of evidence, request for urgent cross-border operations or surveillance

2. INFORMATION SYSTEMS

2.1. The Schengen Information System – Second Generation (SIS II)[33]

Currently, the second generation Schengen Information System ('SIS II') is operational in 26 EU Member States as well as in the four non-EU countries that are associated with Schengen cooperation: Norway, Iceland, Switzerland and Liechtenstein. It supports operational cooperation between police authorities and judicial authorities in criminal matters. As SIS is both a police cooperation and border control system, designated police officers, border guards, customs officers, and visa and judicial authorities throughout the Schengen area may consult the SIS. [34]

SIS II data can be searched (subject to strict data protection rules) 24/7 via access points in SIRENE bureaux, at border control points, within national territory and in consulates abroad. The database registers data on both **persons** and **objects** and allows the exchange of data for the purposes of crime prevention and combating irregular immigration. Through SIS online searches, the examining officer rapidly establishes, on a 'hit/no hit'-basis, whether a person being checked is mentioned in the database or not.

Data are referred to as alerts which contain only the information necessary to identify a person or an object and for the action to be taken. The single network of national SIRENE Bureaux ensure the exchange of supplementary information in accordance with the provisions of the SIRENE manual. An alert is a set of data enabling authorities to identify persons or objects with a view to taking appropriate action:

---

33 Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ, L 205/63, 7.8.2007.

34 A list of the national competent authorities which have the right to access alerts is published annually in the *Official Journal of the European Union*.

Alerts on **persons**, targeting both EU citizens and non-EU citizens. These facilitate measures such as:

– arrest for surrender purposes on the basis of either the European Arrest Warrant or agreements concluded between the EU and third countries, or for extradition purposes;

– search for the whereabouts of missing persons;

– summons to appear before a court of justice in the context of a penal procedure or of the execution of a sentence involving deprivation of liberty;

– discreet watch and specific checks with a view to repression of penal offences, prevention of threats to public security or prevention of threats to national security;

– refusal of entry into the Schengen territory for nationals or aliens as a result of an administrative or judicial decision or on grounds of threat to public order or to national safety and security, or on grounds of non-observance of national regulations for entry and abode of foreigners.

SIS II alerts on **objects** are entered for discreet or specific checks, for the purpose of seizure, use as evidence in criminal proceedings or surveillance. These alerts can relate to:

– vehicles, boats aircrafts, containers

– firearms

– stolen documents

– banknotes

– stolen property such as art objects, boats, ships.

Specifically authorised Europol staff have the right, within the scope of their mandate, to access and search directly data entered into SIS II and may request further information from the Member State concerned.

The national members of Eurojust and their assistants have the right, within the scope of their mandate, to access and search data entered into SIS II.

Three years after SIS II was brought into operation, the Commission carried out an evaluation of the system. The three recent new SIS Regulations (SIS recast) take account of that evaluation and aim at an increased efficiency in the fight against terrorism and serious crime, in particular through improved information exchange between competent authorities. Furthermore, they support border and migration management and prepare the SIS for interoperability with large-scale EU information systems, such as VIS, Eurodac, ETIAS and EES. The Regulations, amending the legal and operational framework of the SIS II, are:

- Regulation (EU) 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals[35];

- Regulation (EU) 2018/1861 on the establishment, operation and use of the SIS in the field of border checks[36]; and

- Regulation (EU) 2018/1862 on the establishment, operation and use of the SIS in the field of police cooperation and judicial cooperation in criminal matters[37].

35 Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, OJ L 312/1, 7.12.2018.

36 Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L 312/14, 7.12.2018.

37 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312/56, 7.12.2018.

The 3 revised SIS Regulations entered into force in December 2019 and they will be completely operational as of December 2021. The new functionalities in SIS are being implemented in different stages, with a requirement for the work to be completed by 2021. An AFIS (Automated Fingerprint Identification System) was introduced in March 2018 in SIS, making it possible to carry out searches using fingerprints as of 2021.

The regulations contain specific rules for those Member States which have a special status regarding Schengen and measures in the area of freedom, security and justice of the TFEU, e.g. Denmark, Ireland, Croatia, Bulgaria, Romania, and Cyprus. Furthermore, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1860 provide the legal basis for the European Border and Coast Guard (EBCG) Team Members for directly accessing SIS data for the purpose of border checks and of return of illegally staying third-country nationals. Within their mandate and provided that they are authorised to carry out checks and have received the required training, the EBCG Team Members shall exercise the right through a technical interface, which is to be set up and maintained by the European Border and Coast Guard Agency (Frontex) and shall allow direct connection to the Central SIS II.

2.2. EIS – The Europol Information System[38]

The Europol Regulation introduces a new concept for data processing, which is commonly referred to as the Integrated Data Management Concept (IDMC). IDMC can be defined as the possibility to use crime related information for multiple business purposes as indicated by the data owner, allowing for its management and processing in an integrated, technology-neutral manner. Under the Europol Council Decision, the processing of data was structured around systems. The Europol Regulation no longer contains references to systems, but instead requires the indication of processing purposes. To facilitate a smooth transition, users can continue to work with the existing systems in a way that complies with the new legal framework.

[38] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114 (applicable as from 1 May 2017)

The Europol Information System (EIS), referred to in the Europol Decision, is a centralised system hosted by Europol which allows Member States and Europol's cooperation partners to store, share and cross-check data related to suspects, convicts or 'potential future criminals' involved in crimes falling within Europol's mandate (serious crime, organised crime or terrorism). It allows storage of the entire range of data and evidence related to those crimes/persons e.g. persons with aliases, companies, telephone numbers, email addresses, vehicles, firearms, DNA, photo, fingerprints, bombs etc. The EIS, which serves in first instance as the system supporting cross-checking, provides a hit/not hit access. The Europol Regulation foresees full access to data submitted for strategic-thematic analysis, but only access on a hit/no hit basis for data that is contributed for operational analysis.

The EIS is de facto a reference system which helps to identify whether or not information searched for is available in one of the EU Member States, from cooperation partners or at Europol. It is directly available in all Member States and to duly authorised Europol staff. At present, three ways of uploading data by Member States can be distinguished:

(a) manual insertion of data in EIS or through SIENA;

(b) semi-automated transfer by conducting a batch up-load in EIS;

(c) automated data transfer, using a dataloader.

The vast majority of data in the Europol Information System (EIS) is entered by means of automated data loading systems. The data collection approach by Member States has changed, with the focus on transmitting data shifting to entities that can be cross-matched such as persons, cars, telephone numbers and firearms.

Third countries cannot directly enter nor cross-check data in the EIS, but in accordance with Article 23(5) of the Europol Regulation they may send it to Europol. Europol will first need to assess whether that data falls within its mandate and only then accept the data and carry out the cross-checking of data.

The EIS, which allows the sharing of highly sensitive information, has a robust system ensuring confidentiality and security. Security is ensured, for instance, by the specific handling codes. They indicate what can be done with the given information and who has access to it. The handling codes are designed to protect the information source and ensure that processing the information is in accordance with the wishes of the owner of the information and in accordance with the national law of the Member State. The EIS is accredited for the processing of data up to and including EU RESTRICTED.

2.3. SIENA - Europol's Secure Information Exchange Network Application

SIENA is Europol's secure communication system for use by Member States, Europol and its cooperation partners to exchange operational and strategic crime-related information and intelligence, including operational data on persons. SIENA is a messaging system offering different message types for different purposes,

In the design and functioning of SIENA, significant emphasis was placed on security, data protection and confidentiality. SIENA has been accredited for the exchange of EU CONFIDENTIAL information. Data exchange via SIENA implies clear data processing responsibilities. For each SIENA message sent out, the classification (confidentiality), handling codes and reliability of the source and information must be indicated.

The default language of the SIENA user interface is English while the interface is multilingual, enabling the SIENA operators to work in their own national language(s). In addition to exchanging messages, SIENA operators can perform searches and create statistical reports on the data exchanged via SIENA.

SIENA supports bilateral data exchange between Member States and allows them to exchange data outside of the Europol mandate. When addressing one of Europol's cooperation partners in the data exchange, Member States are notified via SIENA that this exchange should only take place if it concerns crimes within Europol's mandate.

Europol will only handle the information exchanged via SIENA for operational data processing purposes if Europol is included as an addressee in the data exchange. For auditing purposes, all data exchanged via SIENA is available to the Europol Data Protection Officer and the national supervisory bodies.

SIENA supports the structured data exchange based upon the Universal Message Format (UMF). Currently, the entities can be created/shown in the SIENA web application itself. The complete UMF data model is already supported by the SIENA web service.

2.4. I-24/7 - Interpol's global police communications system

The I-24/7 global network for the exchange of police information connects the Interpol General Secretariat in Lyon, France, the National Central Bureaux (NCB) in 190 countries and regional offices.

The Interpol Information System enables direct message communication between NCBs. All Interpol databases (except the database of child sexual exploitation images) are accessible in real time via the I-24/7 global police communications system. The I-24/7 system also enables Member countries to access one another's national databases using a business-to- business (B2B) connection. Member countries manage and maintain their own national criminal data and control its submission, access by other countries and the destruction of data in accordance with their national laws. They also have the option to make it accessible to the international law enforcement community through I-24/7.

2.4.1. Interpol: DNA Gateway

The Interpol DNA database includes an international DNA database, an international search request form for bilateral exchange and a means for secure standardised electronic transfer. No nominal data are kept that link a DNA profile to any individual. The DNA Gateway is compatible with Prüm automated data exchange.

Member countries can access the database and, upon request, access can be extended beyond the member countries' National Central Bureaux to forensic centres and laboratories. Police in member countries can submit a DNA profile from offenders, crime scenes, missing persons and unidentified bodies.

2.4.2. Interpol Fingerprint Database

Authorised users in member countries can view, submit and cross-check records via an automatic fingerprint identification system (AFIS). Records are saved and exchanged in the format defined by the National Institute of Standards and Technology (NIST). The Guidelines concerning Fingerprints Transmission and the Guidelines concerning transmission of Fingerprint Crime Scene Marks assist Member Countries in improving the quality and quantity of fingerprint records submitted to the Interpol AFIS.

2.4.3. Interpol Stolen and Lost Travel Documents database

Interpol's Stolen and Lost Travel Documents database holds information on more than 45 million travel documents reported lost or stolen by 166 countries. This database enables Interpol NCBs and other authorised law enforcement bodies (such as immigration and border control officers) to ascertain the validity of a suspect travel document. For the purpose of preventing and combating serious and organised crime, Member States' competent law enforcement authorities exchange passport data with Interpol.[39]

2.4.4. Travel Documents Associated with Notices (TDAWN)

The TDAWN database contains information on travel documents linked to individuals who are subject to an INTERPOL notice.

2.4.5. Firearms Reference Table

The INTERPOL Firearms Reference Table allows investigators to properly identify a firearm used in a crime (its make, model, calibre, etc.). It contains more than 250 000 firearms references and 57 000 high-quality images. The INTERPOL Ballistic Information Network is a platform for the large-scale international sharing and comparison of ballistics data, and has more than 150 000 records.

The Interpol Illicit Firearms Records and Tracing Management System (iARMS) is an information technology application which facilitates information exchange and cooperation between law enforcement agencies on firearms-related crime.

---

[39] Council Common Position 2005/69/JHA on exchanging certain data with Interpol, OJ L 27/61, 29.1.2005.

2.5. ECRIS[40]

The IT-based European Criminal Records Information System (ECRIS)[41] provides the electronic means for conviction information to be exchanged between Member States in a standardised format. ECRIS is used to notify Member States about convictions of their nationals and to send requests for conviction information for the purpose of criminal proceedings and other purposes, such as administrative or employment purposes. It is also possible to make requests for third-country nationals, if there is reason to believe that the Member State requested holds information on that person.

ECRIS requests have to be replied to within 10 working days, if the request is for either criminal proceedings or employment purposes, and within 20 working days if the request has originated from an individual for his own information.

ECRIS is not designed to establish any centralised criminal record database and is based on a decentralised IT architecture whereby all criminal records are solely stored in databases operated by Member States. The data is exchanged electronically between the designated Central Authorities of the Member States.

The information is to be transmitted by Member States in accordance with agreed rules and standardised formats, and must be as complete as possible so as to allow the receiving Member State to process the information properly and identify the person. Messages are sent in the official languages of the Member States concerned or in another language accepted by both Member States.

---

40 Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93/23, 7.4.2009.

41 Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, OJ L 171/143, 7.6.2019, OJ L 151/143, 7.6.2019.

A Non-Binding Manual for Practitioners setting out the procedures for information exchange and coordinating their action for the development and operation of ECRIS is published by the Council General Secretariat and is available in electronic format on the website of the Council and at the European Commission-hosted website CIRCABC at https://circabc.europa.eu. Requests for access to the manual should be sent to the Council Secretariat. Requests for access to the restricted Interest Group 'ECRIS Business and Technical Support' should be sent to the European Commission.

2.5.1. ECRIS-TCN[42]

The ECRIS legal framework does not sufficiently address the particularities or requests concerning third-country nationals. Within the Union, information on third-country nationals is not gathered as it is for nationals of Member States - in the Member State of nationality - but only stored in the Member States where the convictions have been handed down. By ECRIS-TCN[43], the central national authority can find out which other Member States hold criminal records information on a third-country national. The ECRIS framework can then be used to request such information from those Member States in accordance with Framework Decision 2009/315/JHA.

The Regulation lays down rules establishing a centralised system at the Union level containing personal data, and rules on the division of responsibilities between the Member State and the organisation responsible for the development and maintenance of the centralised system. It provides for an adequate overall level of data protection, data security and protection of the fundamental rights of the persons concerned.

---

42 Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member Stats holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records System and amending Regulation (EU) 2018/1726, OJ L 135/1, 22.5.2019.
Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, OJ L 171/143, 7.6.2019

43 The Commission will determine the date from which ECRIS-TCN is to start operations once the conditions set out in Article 35 of Regulation (EU) 2019/816 are met.

Member States should create records in ECRIS-TCN regarding convicted third-country nationals. This should, where possible, be done automatically and without undue delay after their conviction was entered into the national criminal records. Member States should, in accordance with the Regulation, enter into the central system alphanumeric and fingerprint data relating to convictions handed down after the date of the start of entry of data into the ECRIS-TCN. As from the same date, and any time thereafter, Member States should be able to enter facial images in the central system.

ECRIS-TCN provides for processing of fingerprint data for the purpose of identifying the Member States in possession of criminal records information on a third-country national. It should also allow for processing of facial images in order to confirm his or her identity. It is essential that the entry and use of fingerprint data and facial images not exceed what is strictly necessary to achieve the aim, respect fundamental rights, as well as the best interests of children, and be in conformity with applicable Union data protection rules.

Eurojust, Europol and the EPPO should have access to ECRIS-TCN for the purpose of identifying the Member States holding criminal records information on a third-country national in order to support their statutory tasks.

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is tasked to develop and operate ECRIS-TCN.

2.6. Visa Information System (VIS)

The authorities designated by the Member States in accordance with the Council Decision 2008/633/JHA[44] may consult the VIS if it is necessary or if there are reasonable grounds for believing that such a search would substantially help in preventing, detecting or investigating of terrorism offences and other serious criminal offences.

Which authorities can consult VIS for law enforcement purposes?

National authorities which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences and designated by the Member States in accordance with the Council Decision 2008/633/JHA. Only duly empowered staff of the operational units within the designated authorities can consult and use information from the VIS for the law enforcement purposes based on the provisions of the Council Decision 2008/633/JHA.

When the Common Identity Repository (CIR) becomes operational, designated authorities may also access VIS for consultation under certain conditions. When designated authorities launch a query in the CIR in accordance with Article 22 of Regulation (EU) 2019/817[45], and where the conditions for access laid down in this Article are met, they may access the VIS for consultation where the reply received as referred to in Article 22(2) of that Regulation reveals that data are stored in the VIS.

Declarations concerning Member States' designated authorities and central access point(s) for access to Visa Information System data for consultation in accordance with Article 3(2) and 3(3) respectively of Council Decision 2008/633/JHA[46].

---

[44] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).

[45] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

[46] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.C_.2013.236.01.0001.01.ENG

Which data could be searched?

Designated authorities can search with any of the following data: surname, surname at birth (former surname(s)); first name(s); sex; date of birth, place and country of birth; current nationality and nationality at birth; type and number of the travel document, the authority which issued it and the date of issue and of expiry; main destination and duration of the intended stay; purpose of travel; intended date of arrival and departure; intended border of first entry or transit route; residence; fingerprints; type of visa and the number of the visa sticker; details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay. Consultation of the VIS shall, in the event of a hit, give access to any other data taken from the application form, photographs, the data entered in respect of any visa issued, refused, annulled, revoked, or extended.

Access to VIS by Europol: Europol designated a specialised unit with duly empowered Europol officials to act as the central access point to access the VIS for consultation in accordance with Council Decision 2008/633/JHA. When CIR becomes operational, in cases where Europol has launched a query of the CIR in accordance with Article 22 of Regulation (EU) 2019/817, and where the conditions for access laid down in this Article are met, Europol may access the VIS for consultation where the reply received as referred to in Article 22(2) of that Regulation reveals that data are stored in the VIS. Europol shall obtain the consent of the relevant Member State in order to process data originating from VIS.

2.7. Schengen Information System (SIS)

The SIS enables competent authorities, such as police, border guards, migration and visa authorities to enter and to consult alerts on wanted or missing persons and objects.

The general purpose of the SIS is to ensure a high level of security within the area of freedom, security and justice of the Union and law enforcement authorities can access the SIS for all police checks and the right of access covers all types of alerts. Therefore, the SIS access is different from the 'law enforcement access' to other databases as law enforcement is the core business of the SIS and law enforcement authorities are among its intended end-users, hence there are no specific conditions to search SIS alerts, including the 'migration related' alerts.

What types of 'migration related' alerts exist in SIS?

'Alerts on return' - Article 3 of Regulation (EU) 2018/1860[47]

This alert category concerns irregularly staying third-country nationals subject to a return decision, which imposes an obligation to return to their country of origin or another third country. The alert on return in SIS is issued to verify that the obligation to return has been complied with. Alerts on return include information on whether the return decision is accompanied by an entry ban, and, where relevant, whether the decision is issued in relation to a third-country national who poses a threat to public policy, to public security or to national security ('security flag').These alerts are issued by migration authorities.

'Alerts for refusal of entry and stay' - Articles 24 and 25 of Regulation (EU) 2018/1861[48]

This alert category concerns third-country nationals who are not entitled to enter into and stay in the Schengen area, including due to previous conviction, because they pose a serious security threat, due to circumvention of Union or national law on entry and stay, entry bans or due to restrictive measures. Alerts for refusal of entry and stay include information about the reason for the entry ban decision, for example previous conviction, or serious security threat. These alerts are issued by migration authorities or police authorities (in some cases on behalf of security services).

---

47 Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ L 312, 7.12.2018, p. 1).

48 Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 07/12/2018, p. 14).

Which data can be found in a SIS alert?

SIS alert contains biographic data - information required to identify the person, including all known aliases (name/surname/date of birth/previously used names and aliases/place of birth/nationalities held). It might also contain dactyloscopic data - fingerprints, palm prints, fingermarks and palm marks of the person. The alert also contains case related data, such as the type of offence and action to be taken. All alert categories may also include warning markers (e.g. that the subject of the alert is armed, violent, or is involved in terrorism-related activity). The authorities can search the SIS based on alphanumeric data (name/surname/date of birth) or solely on the basis of the fingerprints.

Which authorities can access data in SIS?

National competent authorities have access to data entered in SIS for border control, police and customs checks, examining visa applications, taking decisions related to the entry and stay of third-country nationals. This includes a number of authorities, including national judicial authorities.

The renewed SIS legal framework, applicable since March 2023, has extended the access rights of national authorities. It is explicitly provided that in addition to police checks, national authorities responsible for the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies, have access to SIS data. Migration authorities have now the right to access all types of alerts in SIS.

In addition, Europol and the European Border and Coast Guard teams, teams of staff involved in return-related tasks, and members of the migration management support teams also have access to all SIS alert categories including the ‘migration related’ alerts.

The detailed list of competent authorities in each Member State authorised to search the data contained in SIS is maintained by eu-LISA[49].

[49] SIS LoA, N.SIS, SIRENE 2023.pdf

2.8. Eurodac

It is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in Eurodac is necessary for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences. Therefore, the data in Eurodac is available, subject to the conditions set out in Regulation (EU) 603/2013[50] (current) or Regulation (EU) 2024/1358[51] (Eurodac recast), for comparison by the designated authorities of Member States and Europol. Eurodac recast Regulation (EU) 2024/1358 is not applicable yet and will start to apply from 12 June 2026.

Which authorities can consult Eurodac for law enforcement purposes?

National authorities which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences and are designated by the Member State to request comparisons with Eurodac data pursuant to the Regulation (EU) 603/2013 (current) or Regulation (EU) 2024/1358 (Eurodac recast).

---

50 Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) (OJ L 180, 29.6.2013, p. 1)

51 Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of 'Eurodac' for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council (OJ L, 2024/1358, 22.5.2024)

Which data could be searched?

Recast: Requests for comparison with Eurodac data for law enforcement purposes can be carried out with biometric or alphanumeric data.

Current: Those requests can only be carried out with fingerprint data.

Procedure to consult for law enforcement purposes

Recast: The Regulation (EU) 2024/1358 sets out that designated authorities may only access Eurodac if a prior check on national fingerprint databases and automated fingerprinting identification systems of all other Member States via Prüm has returned a negative result. If there are reasonable grounds that searches via Prüm will not lead to the identification of a person this check is not necessary. In addition to these prior checks, designated authorities may also conduct a search in VIS which can be submitted simultaneously with the request for Eurodac.

Where the designated authorities have consulted the CIR in accordance with Article 22(1) of Regulation (EU) 2019/818[52] and it was indicated that there is relevant data stored in Eurodac, the designated authorities may access Eurodac for consultation without these prerequisites.

Current: The above-mentioned procedure for access to Eurodac under current Regulation (EU) 603/2013 is similar with the negative check in VIS being mandatory and previous consultation of CIR not being available to circumvent the cascade.

Access to Eurodac by Europol

Europol designated authorities shall be authorised to request comparisons with Eurodac data for the same reasons as Member States and if prior searches in all technically and legally available systems did not lead to an identification. Processing of information obtained from comparison with Eurodac data is subject to the authorisation of the Member State owning the data.

---

52 Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).

2.9. Entry Exit System (EES)

Which authorities can consult EES for law enforcement purposes?

National authorities which are designated by Member States pursuant to Article 29 of Regulation (EU) of Regulation (EU) 2017/2226[53] are entitled to consult the EES data for prevention, detection and investigation of terrorist offences or other serious criminal offences. The conditions for access to EES data by designated authorities are specified in Article 32 of the Regulation. Access is permitted if it is necessary for preventing, detecting, or investigating terrorist offenses or other serious criminal offenses, is necessary and proportionate in a specific case, and if there is evidence or reasonable grounds to believe that accessing EES data will contribute to these objectives. This is particularly relevant when there is a substantiated suspicion that the suspect, perpetrator, or victim falls under a category covered by the Regulation (EU) 2017/2226.

Which data could be searched?

Consultation of the EES for the purpose of identification is limited to searching in the individual file with any of the following EES data: fingerprints of visa-exempt third-country nationals or of holders of a Facilitated Transit Document. In order to launch this consultation of the EES, latent fingerprints may be used and may therefore be compared with the fingerprints stored in the EES as well as facial images.

---

53 Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20)

Procedure to consult EES for law enforcement purposes

Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence is allowed after a prior search has been conducted in national databases and, in the case of searches with fingerprints, a prior search has been launched in the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA where comparisons of fingerprints are technically available, and either that search has been fully carried out, or that search has not been fully carried out within two days of being launched. Exceptions to the general conditions are made in cases of urgency where there is a need to prevent an imminent danger to the life of a person.

Access to EES by Europol

Europol must designate one of its operating units as the 'Europol designated authority' and authorise it to request access to the EES through the Europol central access point. One of the conditions for Europol access is that the consultation would need to be necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offence falling under Europol's mandate. Access to EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim is allowed where the consultation, as a matter of priority, if the data stored in the databases that are technically and legally accessible to Europol have not made it possible to identify the person in question.

2.10. European Travel Information and Authorisation System (ETIAS)

Which authorities can consult ETIAS for law enforcement purposes?

Member States' designated authorities and Europol may consult data stored in the ETIAS Central System for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences falling under their competence under the conditions established in the Regulation (EU) 2018/1240[54].

[54] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1)

Which data could be searched?

Consultation of the ETIAS Central System is possible with one or several of the following items of data recorded in the application file: surname (family name) and, if available, first name(s) (given names); other names (alias(es), artistic name(s), usual name(s)); number of the travel document; home address; email address; phone numbers; IP address. Consultation may be combined with the following data in the application file to narrow down the search: nationality or nationalities, sex, date of birth or age range.

Procedure to consult ETIAS for law enforcement purposes

An operating unit within the designated authorities that are authorised to request a consultation of data stored in the ETIAS Central System can submit a reasoned request for consultation of a specific set of data stored in the ETIAS Central System. Each Member State shall designate a central access point which shall have access to the ETIAS Central System. The central access point shall verify that the conditions to request access to the ETIAS Central System are fulfilled. If the conditions for access are fulfilled, the central access point shall process the request. The data stored in the ETIAS Central System accessed by the central access point shall be transmitted to the operating unit that made the request in such a way that the security of the data is not compromised. In a case of urgency, where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or other serious criminal offence, the central access point shall process the request immediately and shall only verify ex post whether all the conditions are fulfilled, including whether a case of urgency actually existed. The ex post verification shall take place without undue delay and in any event no later than seven working days after the processing of the request.

Access to ETIAS by Europol

Europol may request to consult data stored in the ETIAS Central System and submit a reasoned electronic request to consult a specific set of data stored in the ETIAS Central System to the ETIAS Central Unit.

2.11. Future query in the Common Identity Repository (CIR)

Article 22 of Regulation (EU) 2019/817 and Regulation (EU) 2019/818 (Interoperability Regulations) will make it possible for the Member States' designated authorities and Europol to query the Common Identity Repository (CIR) for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences (so-called first step of the law enforcement access).

The idea behind the query of the CIR is to enable designated authorities and Europol, before requesting full access to data stored in the system(s) through central access points, to verify whether any of the systems (ETIAS, EES, VIS and Eurodac) contains data on the person concerned.

In reply to the query in the CIR, designated authorities or Europol will receive a match or no match reply. In case of match(es), designated authorities or Europol will receive a reference(s) to the EU information system(s) that contains data about the person, e.g. match, data can be found in VIS and Eurodac. No other data will be returned. On the basis of this information, designated authorities and Europol can request full access to data stored in the systems according to the rules laid down in the Regulations establishing the underlying systems (so called second step of the law enforcement access as described above).

2.12. CIS – Customs Information System[55]

The Customs Information System complements the Naples II Convention[56]. The system aims at enhancing Member States' customs administration through rapid information exchange with a view to preventing, investigating and prosecuting serious violations of national and Community law. The CIS also establishes a customs file identification database (FIDE) to assist customs investigations.

---

55 Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, OJ L 323/20, 10.12.2009.

56 Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations, OJ C 24/2, 23.1.1998.

The CIS, managed by the Commission, is a centralised information system accessible via terminals in each Member State and at the Commission, Europol and Eurojust. National customs, taxation, agricultural, public health and police authorities, Europol and Eurojust may access CIS data. Only the authorities designated by the Member States [57]and the Commission have direct access to the data contained in the CIS. In order to enhance complementarity, Europol and Eurojust have read-only access to the CIS and to FIDE.

The CIS comprises personal data with reference to commodities, means of transport, business, persons and goods and cash retained, seized or confiscated. Personal data may only be copied from CIS to other data-processing systems for risk management or operational analyses, which only the analysts designated by the Member States may access.

FIDE enables national authorities responsible for conducting customs investigations, when they open an investigation file, to identify other authorities that may have investigated a given person or business.

2.13. False and Authentic Documents Online - FADO[58]

A computerised image archiving system comprising false and authentic documents and based on internet technology enables fast and secure information exchange between the General Secretariat of the Council of the European Union and document checkers in all Member States, as well as in Iceland, Norway and in Switzerland. The system enables an on-screen comparison between the original and a false or forged document. Primarily, it contains documents of the Member States as well as documents of third countries from where there are regular immigration flows to the Member States. The database established by FADO includes the following data:

- images of genuine documents
- information on security techniques (security features)
- images of typical false and forged documents

---

57 Implementation of Article 7(2) and Article 8(3) of Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes - updated lists of competent authorities, 13394/11 ENFOCUSTOM 85.

58 Joint Action (98/700/JHA) of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning the setting up of a European Image Archiving System (FADO), OJ L 333/4, 9.12.1998.

- information on forgery techniques, and
- statistics on detected false and falsified documents and identity fraud

The system uses special data lines between the General Secretariat of the Council and the central services located in the Member States. Within each Member State, the system is read through a secure internet connection from a central service. A Member State may use the system internally on its own territory, which means connecting different stations at its various border control posts or other competent authorities. However, there is no direct link between a workstation, other than the national central service, and the central point in the General Secretariat.

FADO is currently available in 22 official languages of the European Union. Documents are introduced by document experts in any of the languages and the standardised descriptions are translated automatically. Accordingly, documents are immediately available in all supported languages. Additional free text information contained is translated subsequently by specialised linguists in the General Secretariat of the Council.

2.14. Public Register of Authentic Travel and Identity Documents Online - PRADO

While access to FADO is restricted to document checkers and for governmental use, the Council of the European Union **P**ublic **R**egister of **A**uthentic Travel and Identity **D**ocuments **O**nline (PRADO) contains a subset of FADO information made available to the general public. The website[59] is published in the official languages of the EU by the General Secretariat of the Council of the European Union for transparency reasons and provides an important service to many users in Europe, especially to non-governmental organisations with a need or legal obligation to check identities.

The website contains technical descriptions, including information on security features, of authentic identity and travel documents. The information is selected and provided by document experts in the Member States, Iceland, Norway and Switzerland.

In PRADO, users can also find links to websites with information on invalid document numbers provided by some Member States as well as third countries and other useful information related to identity and document checking and fraud.

[59] http://www.prado.consilium.europa.eu/

2.15. Summary Overview of Information Systems used for EU Information Exchange

IT Systems & Databases	Legal basis	Purpose	Data Subjects	Data sharing
Second Generation Schengen Information System - **SIS II**	Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) OJ L 205/63, 7.8.2007	• Internal security • Border control • Judicial cooperation • Investigation of crime	• EU citizens • Third-country nationals	• VIS • Europol • Eurojust • Interpol
	Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) OJ L 381/4, 23.12.2006	• Refusing entry or stay • Asylum, immigration and return policies	• Third-country nationals not enjoying rights of free movement equivalent to those of EU citizens	
	Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 OJ L 312/14, 7.12.2018	• Refusing entry or stay • Border control • Investigation of crime	• Third-country nationals	• Europol • European Border and Coast Guard (Frontex)

	Regulation 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals OJ L 312/1, 7.12.2018	• Migration and return policies	• Third-country nationals	• Europol • European Border and Coast Guard (Frontex)
	Regulation 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU OJ L 312/56, 7.12.2018	• Internal security • Border control • Judicial cooperation • Investigation of crime		
Europol **EIS**	Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), Articles 11 to 13 OJ L 121/37, 15.5.2009	• Serious crime • Immigration • Internal security • Counterterrorism	• EU citizens • Third-country nationals	• SIS II
Interpol **I-24/7**	Interpol Constitution		• EU citizens • Third-country nationals	• SIS II • Europol • VIS

Interpol **Lost/Stolen Travel Documents (LSTD)**	Council Common Position 2005/69/JHA on exchanging certain data with Interpol OJ L 27/61, 29.1.2005	• International and organised crime • Internal security	• EU citizens • Third-country nationals	
ECRIS	Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA OJ L 171/143, 7.6.2019	• Criminal proceedings	• EU citizens • Third-country nationals	
ECRIS-TCN	Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member Stats holding conviction information on third-country nationals and stateless persons (ECIS-TCN) to supplement the European Criminal Records System and amending Regulation (EU) 2018/1726 OJ L 135/1, 22.5.2019 Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA OJ L 171/143, 7.6.2019	• Criminal proceedings	• Third-country nationals	• Europol • Eurojust • EPPO

VIS	Council Decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC), OJ L 213/5, 15.6.2004 Council Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences, OJ L 218/129, 13.8.2008 Council Decision fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, (2013/392/EU), OJ L 198/45, 23.7.2013	• Serious crime • Internal security • Counterterrorism	• Third-country nationals	• SIS II • Europol • Interpol

Eurodac	Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) OJ L 180/1, 29.06.2013 Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person OJ L 180/31, 29.6.2013	• Immigration • Serious crime • Internal security • Counterterrorism	• Third-country nationals	• Europol

Passenger Name Record (PNR)	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime OJ L 119/132, 4.5.2016	• Serious crime • Internal security • Counterterrorism	• EU citizens • Third-country nationals	• Europol
Advance Passenger Information (API)	Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data OJ L 261/24, 6.8.2004	• Border control • Immigration	• Third-country nationals	
ETIAS	Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226[60] OJ L 236/1, 19.9.2018 Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS) OJ L 236/72, 19.9.2018	• Border control • Immigration • Serious crime • Internal security • Counterterrorism	• Third-country nationals	• SIS • VIS • EES • Eurodac • Europol • Interpol • ETIAS watchlist

[60] The Commission will determine from when ETIAS is to start operations once the conditions set out in Article 88 of the Regulation are met.

EES	Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry / Exit System OJ L 327/1, 9.12.2017 Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and EU No 1077/2011[61] OJ L 327/20, 9.12.2017	• Border management • Serious crime • Counterterrorism	• Third-country nationals	• VIS • Europol • Prüm Decision
CIS	Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes OJ L 323/20, 10.12.2009	• Fight against illicit trafficking	• European citizens • Third-country nationals	• Europol

[61] The Commission will determine from when EES is to start operations once the conditions set out in Article 66 of the Regulation are met.

FADO	Joint Action (98/700/JHA) of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning the setting up of a European Image Archiving System (FADO) OJ L 333/4, 9.12.1998	• Fight against false documents • Immigration policy • Police cooperation	• European citizens • Third-country nationals	

3. LEGISLATION – THE LEGAL CONTEXT, RULES AND GUIDELINES RELATED TO THE MAIN COMMUNICATION METHODS AND SYSTEMS

3.1. Data Protection Directive[62]

Directive (EU) 2016/680, known as the Law Enforcement Directive (LED), establishes specific rules regarding the protection of natural persons, irrespective of their nationality or residence, in relation to the processing of personal data by police and law enforcement authorities. The directive facilitates the exchange of personal data within the EU among competent authorities for the purposes of preventing, investigating, detecting, or prosecuting criminal offences and executing criminal penalties. It aims to ensure a uniform level of protection for individuals by creating legally enforceable rights across the EU. It seeks to prevent divergent practices that could hinder the exchange of personal data among competent authorities.

The Directive offers a comprehensive definition of personal data and processing, seeking to extend its protective measures to all activities involving information related to individuals. Specifically, the term 'personal data' refers to any information that can identify a natural person (data subject), either directly or indirectly. This includes, but is not limited to, names, identification numbers, location data, and other specific characteristics related to an individual's identity, such as physical, physiological, genetic, mental, economic, cultural, or social information. The directive further defines 'processing' in a broad sense, encompassing a wide range of operations performed on personal data. These operations include, but are not limited to, collection, storage, alteration, retrieval, consultation, use, dissemination, and destruction of data, thereby covering every stage of data handling and the exchange of personal data between entities. This inclusive approach ensures robust protection for individuals against any potential misuse or unlawful processing of their personal information.

---

62 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89, 4.5.2016.

The Directive mandates that the processing of personal data adheres to the following principles:

1. Processed Lawfully and Fairly: Data must be collected and subsequently processed in accordance with legal provisions applicable to criminal law enforcement, ensuring that data subjects have a degree of visibility and control over their personal information.

2. Collected for Specified, Explicit, and Legitimate Purposes: Data should be gathered for clearly defined and legitimate reasons and must not be processed in ways that are incompatible with those original purposes.

3. Adequate, Relevant, and Not Excessive: The data collected must be sufficient and pertinent to the purposes for which it is processed, ensuring that unnecessary data is not retained.

4. Accurate and Up to Date: Data should be kept accurate and, where necessary, updated. Reasonable measures must be taken to promptly rectify or erase any inaccurate personal data, considering the purposes for which the data is being processed. This includes the obligation on the authority that provides personal data to another authority, to keep it updated on any changes in the circumstances concerning the data that had been exchanged.

5. Kept in a Form Permitting Identification of Data Subjects: Personal data should only be stored in a manner that allows identification of the data subjects for no longer than necessary for the intended purposes.

6. Processed with Appropriate Security Measures: Data must be handled in a way that guarantees its security, protecting it from unauthorised or unlawful processing as well as from accidental loss, destruction, or damage, through the implementation of suitable technical and organisational safeguards.

The processing of particularly sensitive personal data, which includes information revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data (when used solely for the purpose of identifying a natural person), health-related data, and information regarding a person's sex life or sexual orientation, is permitted only under stringent conditions. Such processing is allowed exclusively when it is deemed absolutely necessary and must be accompanied by appropriate safeguards to protect the rights and freedoms of the data subjects.

Furthermore, the exchange of these categories of sensitive personal data should occur only when essential, taking into account the specific objectives being pursued and the particular circumstances of each case. It is imperative that the associated risks to the rights and freedoms of data subjects are minimised. When conducting such exchanges, it is important to consider the distinctions between various categories of data subjects—such as victims, witnesses, suspects, and convicts—to ensure that their specific rights and sensitivities are adequately respected and protected.

The Directive expressly prohibits decisions that rely exclusively on automated processing, including profiling, if they have adverse legal consequences for the data subject or significantly affect them. Such decisions are only permissible when they are explicitly authorised by law and must incorporate appropriate safeguards to protect the rights and freedoms of the data subject. At a minimum, this includes the right to request human intervention in the decision-making process. Additionally, these provisions are even more rigorous when the automated decision-making involves special categories of personal data.

Additionally, the LED outlines several rights that data subjects possess concerning the processing of their personal data. These rights include the entitlement to be informed about the processing activities affecting their data, the right to access their personal information, the right to have any factually incorrect data rectified, and the right to have unlawfully processed data deleted.

A critical aspect of the directive is the stringent rules on transfers of personal data to third countries. Adding up to these general robust rules is the stipulation that when personal data is made available by a LEA in one member state, the receiving member state is prohibited from transferring that data to a third country without obtaining prior authorisation from the LEA that originally provided the data.

The establishment of national supervisory authorities, empowered to perform their duties with complete independence, is a vital element in safeguarding the rights of individuals regarding the processing of their personal data. These supervisory authorities are entrusted with the responsibility of monitoring the implementation of the provisions set forth by the directive and ensuring their consistent application across the Union. Furthermore, mechanisms are in place to facilitate cooperation among supervisory authorities in different Member States, particularly in situations involving incidents or complaints that affect authorities and data subjects located in multiple jurisdictions.

3.2. The 'Swedish Framework Decision' (SFD)[63]

The Directive on the exchange of information between the law enforcement authorities of Member States has repealed Framework Decision 2006/960/JHA (SFD). The IED lays down the rules under which Member States' law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations. It covers the exchange of information for the purpose of preventing, detecting or investigating criminal offences between the competent law enforcement authorities of different EU Member States.

Rules on requests for information to the Single Points of Contacts include, for instance, the obligation for the submitting authority to carry out a necessity and proportionality test and be ensured that the requested information is available to that other Member State. In addition, the Directive lays down criteria when a request can be considered urgent as well as minimum requirements for the request in order to allow a rapid and adequate processing. Requests can be submitted by Single Points of Contact or designated Member States' law enforcement authorities.

Each Member State must ensure that its Single Point of Contact provides the requested information as soon as possible and in any event within the following time limits, as applicable:

(a) eight hours in the case of urgent requests relating to directly accessible information;

(b) three calendar days in the case of urgent requests relating to indirectly accessible information;

(c) seven calendar days in the case of all other requests.

Deviation from the time limits is possible if a judicial authorisation is needed. In this case, the requested Single Point of Contact must keep the submitting authority updated and provide the requested information as soon as possible after obtaining the judicial authorisation.

---

63 Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386/89, 29.12.2006, corrected by Corrigendum, OJ L 75/26, 15.3.2007.

Regarding the important issue of refusing requests, the Directive first clarifies that refusal should be the exception. Refusal cases are to be specified exhaustively and interpreted restrictively. However, the rules set out in the Directive place an emphasis on the principles of necessity and proportionality, thereby providing safeguards against any misuse of requests for information, including where it would entail manifest breaches of fundamental rights. The Member States, as an expression of their general due diligence, should therefore always verify the compliance of requests submitted to them with the principles of necessity and proportionality and should refuse those requests they find to be non-compliant.

The Directive includes an interesting provision on the language to be used for the exchange of information. Member States shall establish and maintain a list of one or more of the languages in which their single contact point is able to exchange information. This list should include English.

The default channel of communication will be Europol's Secure Information Exchange Network Application (SIENA).

The Directive includes harmonised rules on the establishment or designation, tasks and capabilities of Single Points of Contact as well as their organisation, composition and training. The SPOC must have access to all information available within their Member State, including by having user-friendly access to all relevant Union and international databases and platforms. It must also be ensured that Single Points of Contact carry out their tasks 24 hours a day, 7 days a week and are provided with qualified staff, appropriate operational tools, technical and financial resources, infrastructure, and capabilities, including for translation, necessary to carry out the tasks under the Directive in an adequate, effective and rapid manner.

The SPOC operates a single electronic case management system (CMS). The Directive lays down certain minimum functions and capabilities of such CMS. The CMS is a workflow system allowing Single Points of Contact to manage the exchange of information.

3.3. Schengen Agreement

3.3.1. SIS II and non-SIS II data exchange

The Schengen Agreement signed on 14 June 1985 was supplemented by the Convention implementing the Schengen Agreement (CISA)[64] in 1990 which created the Schengen Area through the abolition of border controls between Schengen states, common rules on visas, and police and judicial cooperation. The CISA establishes a general requirement for police co-operation and entitles police authorities to exchange information within the limits of their respective national legal system.

With the entry into force of the Amsterdam Treaty in 1999, cooperation measures hitherto in the Schengen framework were integrated into the European Union legal framework and Schengen-related matters are now dealt with by the legislative bodies of the EU. The Schengen Protocol annexed to the Amsterdam Treaty laid down detailed arrangements for this integration process.

The Schengen Information System (SIS) was set up pursuant to the provisions of Title IV of the Convention of 19 June 1990. It constitutes an essential tool for the application of the Schengen acquis. It constitutes also a measure aimed at compensating for the absence of internal border controls on persons within the Schengen area through a tool for exchange of information between competent authorities.

The fact that the legal framework governing the SIS currently consists of separate instruments, does not affect the principle that the SIS constitutes one single information system. The three new SIS Regulations do not affect that principle. They aim at creating synergies in the fight against terrorism and serious crime, in particular through improved information exchange between competent authorities. Furthermore, they support border and migration management and prepare the SIS for interoperability with large-scale EU information systems, such as VIS, Eurodac, ETIAS and EES.

---

64 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of border checks at their common borders, OJ L 239/19, 22.09.2000

Legislation

Regulation (EC) 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381/4, 28.12.2006

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ, L 205/63, 7.8.2007.

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312/56, 7.12.2018

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135/27, 22.5.2019

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019

Key Provisions

The Schengen Information System (SIS) is both a police cooperation and border control system and supports operational cooperation between police authorities and judicial authorities in criminal matters. Designated police officers, border guards, customs officers, and visa and judicial authorities throughout the Schengen area may consult the SIS.[65]

[65] A consolidated list of national competent authorities specifying for each authority, which data it may search and for what purposes, is published annually in the Official Journal of the EU pursuant to Article 31(8) of the SIS Regulation and Article 46(8) of the SIS II Decision.

The second generation Schengen Information System ('SIS II') is currently operational in 26 EU Member States as well as in the four non-EU countries which are associated with Schengen cooperation: Norway, Iceland, Switzerland and Liechtenstein.

- Regarding police cooperation, both the United Kingdom and Ireland requested to be authorised to take part in it, but only the United Kingdom has been authorised, in 2015, to upload live data of that part of the SIS[66] on a provisional basis as a first step allowing evaluation to take place before a final "putting into effect" Decision. The United Kingdom and Ireland do not take part in the application of SIS for the purpose of border control.

- Bulgaria, Romania[67] and Croatia[68] apply the provisions of the Schengen acquis relating to police cooperation and border control. They have been given live access to the SIS for the purpose of evaluation of the correct application of the provisions of the Schengen acquis relating to SIS. Once these evaluations have been carried out satisfactorily, a separate Council Decision will set out a date for the lifting of checks at internal borders. Until that date, certain restrictions remain on the use of SIS.

- Cyprus does not yet have access to the SIS.

SIS II data can be searched online (subject to strict data protection rules) 24/7 via SIRENE bureaux, at border control points, inside national territory and abroad in consulates. Data are referred to as alerts, an alert being a set of data enabling authorities to identify **persons,** i.e. European citizens and non-EU citizens, or **objects** with a view to taking appropriate action for the purposes of combating crime and irregular immigration.

---

66 Council Implementing Decision (EU) 2015/215 of 10 February 2015 on the putting into effect of the provisions of the Schengen *acquis* on data protection and on the provisional putting into effect of parts of the provisions of the Schengen *acquis* on the Schengen Information System for the United Kingdom of Great Britain and Northern Ireland, OJ L 36/8, 12.2.2015.

67 Council Decision of 29 June 2010 on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Bulgaria and Romania 2010/365/EU, OJ L 166/17, 1.7.2010.

68 Council Decision (EU) 2017/733 of 25 April 2017 on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Croatia, OJ L 108/31, 26.4.2017.

Specifically authorised staff of Europol have the right, within the scope of its mandate, directly to access and search data entered into SIS II and may request further information from the Member State concerned.

The national members of Eurojust and their assistants have the right, within the scope of their mandate, to access and search data entered into SIS II.

According to Article 47 of CISA, liaison officers seconded to police authorities in other Schengen States or third countries are responsible for exchanging information pursuant to:

- Article 39(1), (2) and (3) in compliance with national law for the purpose of preventing and detecting criminal offences;

- Article 46, even on their own initiative, for the purpose of preventing offences against or threats to public order and security.

It should be noted that the provisions of Article 39(1), (2) and (3**)** and Article 46, insofar as they relate to the exchange of information and intelligence with regard to serious crime, are replaced by those of Council Framework Decision 2006/960/JHA, the 'Swedish Framework Decision'. However, the provisions of Article 39(1), (2) and (3) and Article 46 remain applicable with regard to offences punishable by a term of imprisonment of less than 12 months.

3.3.2. Schengen Information System recast

Legislation

Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, OJ L 312/1, 7.12.2018

Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L 312/14, 7.12.2018

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312/56, 7.12.2018

Key provisions

Three years after SIS II was brought into operation, the Commission carried out an evaluation of the system. The SIS II recast takes account of that evaluation and of the distinct EU Member States' participation in EU policies in the Area of Freedom, Security and Justice. The three Regulations introduce a series of improvements to SIS which will increase its effectiveness, strengthen data protection and extend access rights. Furthermore, they support border and migration management and pave the way to SIS interoperability with large-scale EU information systems[69].

[69] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019

The regulations contain specific rules as regards those Member States having a special status with Schengen and measures in the area of freedom, security and justice of the TFEU, i.e. Denmark, Ireland, Croatia, Bulgaria, Romania, and Cyprus.

Provisions with regard to Regulation 2018/1862 on the operation and use of the SIS for police and judicial cooperation in criminal matters refer, in particular, to:

- New alert categories, both on persons, such as 'unknown wanted persons' and 'inquiry check', the extension of the category 'missing persons' to 'vulnerable persons who need to be prevented from travelling', and on objects, such as 'objects of high value';
- Obligations for Member States to create SIS alerts for cases related to terrorist offences;
- Rules to inform Europol on hits alerts linked to terrorist offences;
- Rules on the use, for identification purposes, of biometric data, such as facial images and photographs when technically possible[70], fingerprints, palm prints, and, in particluar DNA profiles only for the identification of missing persons;
- Law enforcement access rights with regard to immigration authorities, boat and aircraft registration authorities, services responsible for registering firearms; to Europol to give it full access to SIS, including missing persons, return alerts, and alerts in relation to third-country nationals, and to exchange and further request supplementary information in accordance with the provisions of the SIRENE Manual; to the European Borders and Coast Guard Agency (Frontex) and its teams, insofar as it is necessary for the performance of their tasks and as required by the operational plan for a specific border guard operation.

[70] Facial images and photographs should, for identification purposes, initially be used only in the context of regular border crossing points. Such use should be subject to a report by the Commission confirming the availability, reliability and readiness of the technology. At a later stage, the Commission might adopt acts in respect of the determination of the circumstances in which photographs and facial images may be used for the identification of persons other than in the context of regular border crossing points.

- Enhanced data protection and data security through introducing additional safeguards to ensure that the collection and processing of, and access to, data is limited to what is strictly necessary and operationally required; through application of the EU data protection framework, in particular Directive 2016/680 and the GDPR, is applicable; through coordination and end-to-end supervision by the national data protection authorities and the European Data Protection Supervisor.

3.4. Europol

Legislation

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114 (applicable as from 1 May 2017).

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135/27, 22.5.2019.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019.

Key provisions

The objective of Europol is to support and strengthen action by the Member States' competent authorities responsible for preventing and combating crime, and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States. To that end, Europol collects, stores, processes, analyses and exchanges information and criminal intelligence.

Each Member State designates a national unit (ENU) functioning as the liaison body between Europol and the competent authorities in the Member States. The ENUs carry out tasks related to the sharing of relevant information and intelligence. Each national unit seconds at least one liaison officer constituting the national liaison bureau at Europol and representing the interests of the national unit. Liaison officers are tasked with information sharing between, on the one hand, the Member States and Europol, and, on the other hand, bilaterally between other countries. These bilateral exchanges can cover crimes beyond the Europol mandate.

The Europol Regulation introduces a new concept for data processing, which is commonly referred to as the Integrated Data Management Concept (IDMC). IDMC can be defined as the possibility to use crime related information for multiple business purposes as indicated by the data owner, allowing for its management and processing in an integrated, technology-neutral manner. Under the Europol Council Decision, the processing of data was structured around systems. The Europol Regulation no longer contains references to systems, but instead requires the indication of processing purposes. To facilitate a smooth transition, users can continue to work with the existing systems in a way that complies with the new legal framework.

The national unit is responsible for communication with the Europol Information System (EIS) used to process the data required for the performance of Europol's tasks. The national unit, liaison officers and duly authorised Europol staff have the right to input data into the systems and retrieve data from them. Information inserted into EIS is in general considered as being provided for the purpose of cross-checking (Article 18(2)(a) of the Regulation) and of strategic/thematic analysis (Article 18 (2)(b) of the Regulation).

3.5. European Border and Coast Guard Agency (Frontex)

Legislation

Regulation (EU) 2019/1896 of 13 November 2019 on the European Border and Coast Guard (OJ L 295, 14.11.2019, p. 1) and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 (applicable as of 4 December 2019).

Regulation (EU) No 1052/2013 establishing the European Border Surveillance System (EUROSUR), provides for "a common framework for the exchange of information and for the cooperation between Member States and Frontex in order to improve situational awareness and to increase reaction capability at the external borders of the Member States of the Union ('external borders') for the purpose of detecting, preventing and combating illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants ('EUROSUR)". The EUROSUR Regulation has been repealed and replaced by Regulation (EU) 2019/1896, which carries revised provisions on EUROSUR.

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135/27, 22.5.2019.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019.

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236/1, 19.09.2018.

Key provisions

The objective of the European Border and Coast Guard (EBCG) is to ensure European integrated border management at the external borders with a view to managing those borders efficiently in full compliance with fundamental rights and to increasing the efficiency of the Union return policy.

The European Border and Coast Guard Agency – Frontex (the Agency) addresses migratory challenges and potential future challenges and threats at the external borders. In view of preventing, detecting and combating cross-border crime at the external borders, it ensures a high level of internal security within the Union in full respect of fundamental rights, while safeguarding the free movement of persons within the Union.

Each Member State designates a national contact point for communication with the Agency on all matters pertaining to the activities of the Agency, without prejudice to the role of the national coordination centres. Member States may designate up to two staff members representing their national contact point to be assigned to the Agency as liaison officers.

Each Member State designates, operates and maintains a national coordination centre which shall coordinate, and exchange information among, all authorities having responsibility for external border control at national level, as well as with the other national coordination centres and the Agency.

The EBCG Regulation establishes EUROSUR as an integrated framework for the exchange of information and for operational cooperation with the EBCG. It aims to improve situational awareness and to increase reaction capability for the purposes of border management, with a view to preventing, detecting and combating illegal immigration and cross-border crime, and to protecting and saving the lives of migrants. The Agency coordinates the EUROSUR Fusion Services in order to supply the national coordination centres, the Commission and itself with information on the external borders and on the pre-frontier area on a regular, reliable and cost-efficient basis.

In implementing the ETIAS Regulation, the Agency will set-up the ETIAS Central Unit. The unit is operational 24/7 and responsible for verifying, in cases where the automated application process has reported a hit, whether the applicant's personal data correspond to the personal data of the person having triggered that hit. Where a hit is confirmed or where doubts remain, the ETIAS Central Unit should initiate the manual processing of the application. In implementing the Interoperability Regulation, for a period of one year following notification by eu-LISA of the completion of the test of the MID and before the start of operations of the MID, the ETIAS Central Unit shall be responsible for carrying out multiple-identity detection using the data stored in the EES, VIS, Eurodac and SIS.

In implementing the European Border and Coast Guard Agency (Frontex) mandate, the Agency explored how information received in advance of arrival (Advance Information) of a traveller at external borders can be used to fine-tune risk traveller analysis. The focus was on exploring existing capabilities and identifying new methods for optimising such analysis, which enhance the border crossing decision-making process while providing greater facilitation to bona fide travellers.

The Advance Information Guidelines contribute to the development of profiles to better detect in advance travellers of interest but also to the building of targeting capabilities. Frontex launched a dedicated training course on Advance Information with a view to support Member States in building harmonised analysis capabilities ('targeting capabilities') for border management purposes.

Additionally, a study launched in January 2020 explores the use of Advance Information on travellers entering the Schengen area via external land and sea borders. One of the main aims of this study is to identify, describe and define best practices related to the collection and processing of such Advance Information.

3.6. Interpol

Legislation

Interpol Constitution[71]

Rules governing the processing of information[72]

Rules on the control of information and access to Interpol's files

Key provisions

The mission of Interpol is to facilitate international police cooperation with a view to preventing and fighting crime through enhanced cooperation and innovation on police and security matters. Action is taken within the limits of existing laws in the Member States and in the spirit of the Universal Declaration of Human Rights. Each of the 190 Member States maintains a National Central Bureau (NCB) staffed by its own highly trained law enforcement officials.

The Interpol Constitution is an international agreement that confirms, as members, the governments of all those countries that participated in its adoption in 1956 and lays down the application procedure for countries that were not members in 1956 to join Interpol.

As the main legal document, the Constitution outlines Interpol's aims and objectives. It establishes the mandate of the organisation to ensure the widest possible cooperation between all criminal police authorities and to suppress ordinary law crimes.

In addition to the Constitution, a number of fundamental texts make up Interpol's legal framework. Several levels of control have been put in place in order to ensure compliance with the rules. These relate to controls by National Central Bureaux (NCB), by the General Secretariat and by the independent monitoring body known as the Commission for the Control of Interpol's Files.

71 http://www.interpol.int/en/About-INTERPOL/Legal-materials/The-Constitution
72 http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts

3.7. Liaison officers

Legislation

Convention implementing the Schengen Agreement of 19 June 1990 (CISA) [73], Article 47

Council Decision 2003/170/JHA of 27 February 2003 on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States[74]

Council Decision 2006/560/JHA of 24 July 2006 amending Decision 2003/170/JHA on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States[75]

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114 (applicable as from 1 May 2017)

Council Decision 2008/615JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210/1, 6.8.2008

Bilateral Agreements

Key Provisions

Article 47 of the CISA provides that Member States 'may conclude bilateral agreements providing for the secondment, for a specified or unspecified period, of liaison officers from one [Member] State to the police authorities of another [Member] State'. Liaison officers are not empowered to execute any police measures autonomously and Article 47 specifies that such secondments are 'intended to further and accelerate cooperation, particularly by providing assistance:

---

73 Convention implementing the Schengen Agreement of 19 June 1990 (CISA), OJ L 239/19, 22.9.2000.

74 Council Decision 2003/170/JHA of 27 February 2003, OJ L 67/27, 12.3.2003.

75 Council Decision 2006/560/JHA of 24 July 2006, OJ L 219/31, 10.8.2006.

a) in the form of the exchange of information for the purposes of combating crime by means of both prevention and law enforcement

b) in executing requests for mutual police and judicial assistance in criminal matters

c) with the tasks carried and by the authorities responsible for external border surveillance.'

More information about such secondments can be found in the 'Football Handbook'[76] and in the Council Recommendation of 6 December 2007 concerning a Handbook for police and security authorities concerning cooperation at major events with an international dimension[77].

The CISA provision that national liaison officers may also represent the interests of one or more other Member States has been further developed by the Council Decision on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States (amended in 2006). Provision has also been made for the improvement of cooperation between liaison officers of different Member States in their place of secondment. In various fora, it has been stressed that this cooperation should be encouraged.

In accordance with the Europol Regulation, each Member State designates a national unit (ENU) which functions as the liaison body between Europol and the Member States' competent authorities responsible for preventing and combating criminal offences. The ENUs carry out tasks related to the sharing of relevant information and intelligence. Each national unit seconds at least one liaison officer constituting the national liaison bureau at Europol and representing the interests of the national unit. Liaison officers are tasked with information sharing between, on the one hand, the national unit and Europol, and, on the other hand, bilaterally between other national units. These bilateral exchanges can cover crimes beyond the Europol mandate.

Council Decision 2008/615JHA ('Prüm Decision') provides in Article 17 and 18 for the secondment of national officers for the purpose of maintaining public order and security and preventing criminal offences.

---

[76] Council Resolution of 3 June 2010 concerning an updated handbook with recommendations for international police cooperation and measures to prevent and control violence and disturbances in connection with football matches with an international dimension, in which at least one Member State is involved, OJ C 165/1, 24.6.2010.

[77] OJ C 314/4, 22.12.2007.

3.8. Prüm Data Exchange

Legislation

- Council Decision 615/2008/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

- Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. (OJ L 210, 6.8.2008)

Key Provisions

Member States reciprocally grant cross-border online access to reference data of designated national DNA analysis files and automated dactyloscopic identification systems (AFIS) as well as to vehicle registration data (VRD) (see Chapter 2 of Council Decision 2008/615/JHA).

Specific NCPs must be designated in each Member State. Data protection and data security provisions must be adequately accounted for in national legislation. The automated comparison of anonymous biometric profiles is based on a hit/no hit system, except in the case of VRD where owner/holder data searched for is automatically returned.

In the event of a biometric match, the NCP of the searching Member State receives, in an automated process, the reference data with which a match has been found.

Additional specific personal data and further information relating to the reference data may then be requested through mutual assistance procedures, including those adopted pursuant to the 'Swedish Framework Decision'.

The supply of such supplementary data is governed by the national law, including the legal assistance rules, of the requested Member State. It is understood that the supply of personal data requires an adequate level of data protection on the part of the receiving Member States.[78]

For the prevention of criminal offences and in the interests of maintaining public order and security for major events with a cross-border dimension, Member States may, both on request and on their own initiative, supply each other with non-personal as well as personal data. To that end, specific national contact points (NCP) are designated (see Chapter 3 of Council Decision 2008/615/JHA).

For the prevention of terrorist offences, Member States may supply each other with personal data under certain circumstances. To that end, specific national contact points are designated (see Chapter 4 of Council Decision 2008/615/JHA).

3.9. Visa Information System (VIS)

Legislation

Council Decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC), OJ L 213/5, 15.6.2004.

Council Decision 2013/392/JHA fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ 2013 L 198, p. 45.[79]

---

78 Council Decision 2008/615/JHA complies with the level of protection designed for the processing of personal data in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, the Additional Protocol of 8 November 2001 to the Convention and the principles of Recommendation No R (87) 15 of the Council of Europe Regulating the Use of Personal Data in the Police Sector.

79 On 16 April 2015, the European Court of Justice annulled Council Decision 2013/392/EU of 22 July 2013 fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences. However, the Court declared that the effects of Decision 2013/392 were to be maintained until the entry into force of a new act intended to replace it.

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135/27, 22.5.2019.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019.

Key Provisions

VIS is a system which enables competent national authorities to enter and update short-stay (so called Schengen) visa data and to consult these data electronically. It is based on a centralised architecture and consists of a central information system, the Central Visa Information System (CS VIS), a national interface in each Member State (NI-VIS), and the communication infrastructure between CS-VIS and NI-VIS. Decision 2008/633/JHA allows the VIS to be used to prevent, detect and investigate terrorist offences and other serious criminal offences. It enables designated law enforcement authorities (such as authorities responsible for tackling terrorism or serious criminal offences e.g. drug trafficking or trafficking in human beings) in the countries of the Schengen Area, and Europol to access the VIS. The national designated authorities must follow a procedure to access the VIS once all conditions for access are fulfilled.

In May 2018, the Commission submitted a legislative proposal amending the VIS Regulation aiming at among other things ensuring interoperability between other databases in the JHA area, registering long-stay visas and residence permits in the VIS. The proposal also incorporates and further develops the access rules of law enforcement authorities to the VIS, while repealing Decision 2008/633/JHA.

The upgraded VIS is not expected to be operational before the end of 2021.

3.10. Eurodac

Legislation

The European Automated Fingerprint Identification System (Eurodac) is a computer system originally to facilitate the effective application of the Dublin Convention. The Dublin Convention, signed on 15 June 1990, was replaced by Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national.

Subsequent to changes made to the Regulations concerning Eurodac, they were recast by

Regulation No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), OJ L 180/1, 29.6.2013;

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135/27, 22.5.2019;

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019;

Key Provisions

Regulation No 603/2013 sets out the purpose of Eurodac and defines the conditions for access by designated national law enforcement authorities and by Europol to Eurodac data for the purposes of the prevention, detection or investigation of terrorist offences[80] or of other serious criminal offences[81].

3.11. Naples II

Legislation

Council Act of 18 December 1997 drawing up, on the basis of Article K.3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations, published in OJ C 24/1 23.1.1998

Key Provisions

Member States mutually assist one another in order to prevent and detect infringements of national customs provisions and prosecute and punish infringements of Community and national customs provisions. In the framework of criminal investigations, the Naples II Convention lays down procedures under which customs administrations may act jointly and exchange data, spontaneously or on request, concerning illicit trafficking activities.

Requests are submitted in writing in an official language of the Member State of the requested authority or in a language accepted by that authority. A form sets out the standard for communication of information. The authorities concerned communicate all information which may assist in preventing, detecting and prosecuting infringements. They exchange personal data, meaning all information relating to a natural person who is identified or identifiable.

In order to provide the assistance required, the requested authority or the competent authority which it has addressed proceeds as though it were acting on its own account or at the request of another authority in its own Member State.

---

80 Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164/3, 22.6.2002).

81 Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ l 190/1, 18.7.2002).

3.11.1. Customs Information System - CIS[82]

The Customs Information System complements the Naples II Convention[83]. The centralised information system is managed by the Commission and aims at enhancing Member States' customs administration through rapid information exchange with a view to preventing, investigating and prosecuting serious violations of national and Community law. CIS also establishes a customs file identification database (FIDE) to assist customs investigations.

The Authorities designated by the Member States[84] have direct access to the data contained in the CIS. In order to enhance complementarity with Europol and Eurojust, both bodies are granted read-only access to CIS and to FIDE.

CIS comprises personal data with reference to commodities, means of transport, business, persons and goods and cash retained, seized or confiscated. Personal data may only be copied from CIS to other data-processing systems for risk management or operational analyses, which only the analysts designated by the Member States may access.

FIDE enables national authorities responsible for conducting customs investigations, when they open an investigation file, to identify other authorities that may have investigated a given person or business.

---

82 Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, OJ L 323/20, 10.12.2009.

83 Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations, OJ C 24/2, 23.1.1998.

84 Implementation of Article 7(2) and Article 8(3) of Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes - updated lists of competent authorities, 13394/11 ENFOCUSTOM 85.

3.12. National Asset Recovery Offices (ARO) and CARIN

Legislation

Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, OJ L 332/103, 18.12.2007

The Camden Assets Recovery Inter-Agency Network (CARIN) was established at The Hague on 22-23 September 2004 by Austria, Belgium, Germany, Ireland, Netherlands and the United Kingdom.

Key Provisions

Following the adoption of Council Decision 2007/845/JHA[85], all Member States have since established and designated asset recovery offices (AROs). They can directly exchange information on matters pertaining to the recovery of assets via the SIENA system. Under the auspices of the EU Commission and Europol, the ARO Network facilitates cooperation between AROs of the Member States and strategic discussion and exchange of best practices. The Europol Criminal Assets Bureau (ECAB) acts as a focal point for asset recovery within the EU.

The provisions laid down in Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union[86] will further enhance the effectiveness of cooperation between the asset recovery offices within the European Union. Member States are called upon to transpose the Directive by 4 October 2016.

---

85 Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, OJ L 332/103, 18.12.2007.

86 Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, OJ L 127/39, 29.4.2014.

The Camden Assets Recovery Inter-Agency Network (CARIN), established in 2004 to support the cross-border identification, freezing, seizure and confiscation of property related to crime, enhances the mutual exchange of information regarding different national approaches extending beyond the EU.

As of 2015, the CARIN Network includes practitioners from 53 jurisdictions and 9 international organisations which serve as contact points for the purpose of rapid cross-border exchange of information, on request or spontaneously. National AROs cooperate among themselves or with other authorities facilitating the tracing and identification of proceeds of crime. While all Member States have established an ARO, major differences exist between the Member States in terms of organisational setup, resources and activities.

Information exchanged may be used according to the data protection provisions of the receiving Member States and is subject to the same data protection rules as if it had been collected in the receiving Member State. Spontaneous information exchange in line with this Decision, applying the procedures and time limits provided for in the Swedish Framework Decision, is to be promoted.

3.13. Financial Intelligence Units (FIU)

Legislation

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 658/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.
OJ L 141/73, 5.6.2015

Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA.
OJ L 186, 11.7.2019, p. 122–137

Key Provisions

Under Directive 2015/849 (The 4th Anti-Money-Laundering Directive - or AMLD, as amended by Directive 2018/843), each Member State shall establish an FIU in order to prevent, detect and effectively combat money laundering and terrorist financing. The FIU as the central national unit shall be responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing. The FIU shall be responsible for disseminating the results of its analyses and any additional relevant information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing. It shall be able to obtain additional information from obliged entities. FIUs shall be able to respond to requests for information by competent authorities in their respective Member States when such requests for information are motivated by concerns relating to money laundering, associated predicate offences or terrorist financing.

Besides the above exchange relating to money laundering and terrorism financing, Directive (EU) 2019/1153 stipulates that each Member State shall ensure that its national FIU is also required to cooperate with designated law enforcement authorities of that state and to be able to reply to their reasoned requests for financial information or financial analysis motivated by concerns relating to the prevention, detection, investigation or prosecution of serious criminal offences, as defined in Annex one to the Europol Regulation (2016/794).

In both cases, the FIU may refuse to provide the information when there are objective grounds for assuming that it would have a negative impact on ongoing investigations or where disclosure of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested.

According to Directive 2015/849 (AMLD), Member States shall ensure that FIUs exchange amongst themselves, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering or terrorist financing and the natural or legal person involved, regardless of the type of associated predicate offences and even if the type of associated predicate offences is not identified at the time of the exchange. An FIU may refuse to exchange information only in exceptional circumstances where the exchange could be contrary to fundamental principles of its national law. Member States shall ensure that the information exchanged pursuant to Articles 52 and 53 is used only for the purpose for which it was sought or provided.

On the top of the exchange between FIUs of different Member States according to Directive 2015/849, Directive 2019/1153 now stipulates that in exceptional and urgent cases, the FIUs are also entitled to exchange financial information or financial analysis that may be relevant for the processing or analysis of information related to terrorism or organised crime associated with terrorism. Directive 2019/1153 also authorises the exchange of information between the FIUs and Europol.

FIU.NET is a decentralised computer network for the exchange of information between FIUs.

FIU.NET, originally intended to strengthen the position of the FIUs, has developed over recent years from a secure basic tool for structured bilateral information exchange to a secure multifunctional tool for multilateral information exchange, with case management features as well as semi-automated standardisation of processes. In FIU.NET, each new feature and automated process is optional, with no strings attached. The individual FIUs can decide which of the possibilities and features offered by FIU.NET to use; they just use the features they feel comfortable with and exclude the ones they do not need or want to use.

3.14. EU/US Terrorist Financing Tracking Programme (TFTP) Agreement

Legislation

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program
OJ L 195/5, 27.7.2010

Key provisions

In the aftermath of 9/11, the EU and the US decided to work closely together and concluded the Agreement on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Financing Tracking Programme (EU-US TFTP Agreement). Pursuant to the Agreement, the US Treasury Department also makes TFTP information available to law enforcement, public security or counter terrorism authorities of the Member States concerned and, if appropriate, to Europol and Eurojust.

The TFTP is equipped with robust control measures to ensure that safeguards, including those on personal data protection, are respected. Data are processed exclusively for the purpose of preventing, investigating, detecting or prosecuting terrorism or its financing. For the purposes of the Agreement, the U.S. Treasury Department may request financial payment messaging and related data stored in the territory of the EU from designated providers of international financial payment messaging services.

The benefit from TFTP data for Member States, Europol and Eurojust is limited by the fact that TFTP cross border payment analysis is exclusively based on FIN (Financial Institution Transfer) messages, a SWIFT message type by which financial information is transferred from one financial institution to another. Other payment methods are not considered. However, the TFTP is the only mechanism which enables, within a very short time period, the mapping and profiling of transactions that are suspected of being related to terrorism or the financing of terrorism for the purposes of enhancing internal security. Owing to greater awareness of the reciprocity clauses in this Agreement, EU authorities are increasingly applying that mechanism so as to benefit from data exchange with the US. It should be noted, in this context, that all requests from EU authorities for searches in the TFTP must meet the requirements of Article 10 of the Agreement.

Although the Agreement does not provide for Member States to request through Europol a search for relevant information obtained through the TFTP, it would be useful, in order to improve the EU's response to terrorism and its financing, for Member States to at least inform Europol in a systematic and timely manner of their direct requests under Article 10. To support Member States in channelling requests for TFTP searches, Europol has set up a single point of contact (SPOC) and with its Analysis Work File (AWF) environment and well established cooperation with the Treasury, it is well placed to handle Member State requests effectively.

3.15. Exchange of information on criminal records (ECRIS)

Legislation

Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93, 7.4.2009, p.23. This Framework Decision repeals Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record, OJ L 322/33, 9.12.2005, p. 33.

Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, OJ L 171/143, 7.6.2019

Key Provisions

Council Framework Decision 2009/315/JHA requires a convicting Member State to transmit, as soon as possible, any convictions entered in their criminal register to the Member State(s) of that person's nationality as well as any alterations or deletions made to that conviction. The Member State of nationality is obliged to store the information for the purposes of retransmission. Any alteration or deletion made in the convicting Member State entails an identical alteration or deletion in the criminal register of the Member States of that person's nationality. Conviction information may be requested from the Member State of the person's nationality for the purposes of criminal proceedings or for any other purposes than criminal proceedings, such as preventing an immediate and serious threat to public security. However, the use of information transmitted under this Decision for purposes other than that of criminal proceedings can be limited in accordance with the national law of the requested Member State and the requesting Member State in order to not compromise the chances of social rehabilitation of the convicted person.

Council Decision 2009/316/JHA defines the ways in which a Member State is to transmit such information. The Council Decision lays down the framework for a computerised system of exchange of information extracted from criminal records. The Central Authorities of each Member State use the special request and reply forms annexed to the Framework Decision through the electronic route described in the legislation.

3.15.1. Exchange of information on criminal records of third-country nationals and stateless persons (ECRIS-TCN)

Legislation

Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member Stats holding conviction information on third-country nationals and stateless persons (ECIS-TCN) to supplement the European Criminal Records System and amending Regulation (EU) 2018/1726, OJ L 135/1, 22.5.2019.

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135/27, 22.5.2019.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019.

Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, OJ L 171/143, 7.6.2019.

Key provisions

The Regulation applies to the processing of identity information of third-country nationals who have been subject to convictions in the Member States. 'Third-country national' means a person who is not a citizen of the Union within the meaning of Article 20(1) TFEU, or who is a stateless person or a person whose nationality is unknown. Criminal records regarding these persons are stored in the convicting Member State. The purpose of ECRIS-TCN[87] is to find out which other Member States hold such criminal records information. The ECRIS framework can then be used to request such information from those Member States in accordance with Framework Decision 2009/315/JHA.

The Regulation lays down rules establishing a system containing personal data, which is developed and maintained by eu-LISA and centralised at the Union level, and rules on the division of responsibilities between the Member State and the organisation responsible for the development and maintenance of the centralised system. It provides for an adequate overall level of data protection, data security and protection of the fundamental rights of the persons concerned.

Eurojust, Europol and the EPPO should have access to ECRIS-TCN for the purpose of identifying the Member States holding criminal records information on a third-country national in order to support their statutory tasks.

[87] The Commission will determine the date from which ECRIS-TCN is to start operations once the conditions set out in Article 35 of Regulation (EU) 2019/816 are met.

3.16. Telecommunication Data Retention

Legislation

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services of public communication networks and amending Directive 2002/58/EC.[88]

Key Provisions

The Directive applies to providers of electronic communication services. The Directive states that providers should retain traffic data and location data as well as the related data necessary to identify the subscriber or user, in order to communicate those data to the competent national authorities on their request. For the purpose of the investigation, detection and prosecution of serious crime, Member States oblige the providers of electronic communications services or of public communication networks to retain the categories of data necessary to identify:

- the source of a communication;
- the destination of a communication;
- the date, time and duration of a communication;
- the type of communication;
- users' communication equipment or what purports to be their equipment;
- the location of mobile communication equipment.

No data revealing the content of the communication may be retained.

[88] The judgment of the Court of Justice of the European Union of 8 April 2014 declared the Directive invalid.

3.17. PNR (Passenger Name Record) Directive

Legislation

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

Key provisions

The directive establishes at Union level a common legal framework for the transfer and processing of PNR data and provides for:

a) the transfer by air carriers[89] of passenger name record (PNR) data of passengers on extra-EU flights. If a Member State decides to apply the directive to intra-EU flights, all provisions shall apply to intra-EU flights as if they were extra-EU flights;

b) the processing of PNR data, including its collection, use and retention by the Member States and its exchange between Member States.

For the purpose of processing PNR data, each Member State establishes or designates a competent authority to act as its passenger information unit (PIU). Two or more Member States may establish or designate a single authority to serve as their common PIU.

PNR data, which are set out in Annex I of the directive, are to be transferred to PIUs to the extent that they are already collected by air carriers in the course of their normal business. Some carriers retain advance passenger information (API) as part of PNR data, while others do not. Irrespective of the way air carriers collect API, they have to transfer API data to the PIUs, which will process them in the same way as PNR data. Annex II of the directive contains the list of "serious offences" within the scope of the directive.

---

[89] The Directive does not affect the possibility of Member States to provide, under their national law, for a system of collecting and processing PNR data from non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services - including the booking of flights - for which they collect and process PNR data, or from transportation providers other than those specified in the Directive, provided that such national law complies with Union law.

The processing of PNR data serves the assessment of passengers prior to their arrival in or departure from a Member State in order to identify persons who require further examination by the authorities competent for preventing, detecting, investigating and prosecuting terrorist offences and serious crime, and, where relevant, by Europol within the limits of its competences and for the performance of its tasks.

To carry out the assessment, PIUs may

(a) compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such databases, or

(b) process PNR data against predetermined criteria.

At domestic level, the PIUs transmit PNR data or the result of their processing to the competent national law enforcement authorities entitled to further examine the file or to take appropriate action for preventing, detecting, investigating and prosecuting terrorist offences and serious crime. While PIUs constitute the main cross-border information exchange channel, the competent authorities may address PIUs from another Member State directly in case of emergency and under well defined conditions.

At Union level, PIUs exchange both PNR data collected from air carriers and the result of processing those data among themselves and with Europol, which is entitled, within the limits of its competences and for the performance of its tasks, to request such data from the PIUs.

PNR data are to be retained in a database at the PIU for a period of five years after their transfer from the Member State of arrival or departure of the flight. However, all PNR data shall be depersonalised after a period of six months. This is to be done by masking out any data element which could serve to identify directly the passenger to whom those data relate. The list of PNR data to be masked out is set out in the directive. After five years, PNR data are to be deleted unless they have been transferred to a competent authority for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime and, in this case, their retention is governed by national law.

In accordance with EU legislation on data protection, the PNR Directive prohibits the processing of sensitive data such as race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

3.18. Advance Passenger Information (API)

Legislation

Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data

Key Provisions

The directive aims at improving border controls and combating illegal immigration. To that end, the directive requires Member States to establish an obligation for air carriers to communicate certain information concerning their travellers in advance of their entering the European Union. Such information is referred to as Advance Passenger Information (API). Under certain conditions and circumstances, Member States may also use API data for law enforcement purposes.

The information is supplied at the request of authorities responsible for carrying out checks on persons at the external borders of the EU.

Air carriers should transmit API data electronically, or, in case of failure, by any other appropriate means, to the authorities carrying out the border checks where the passenger enters the EU. API data are checked against national and European databases such as the Schengen Information System (SIS) and the Visa Information System (VIS).

When API data match an entry in a database (watchlist), an alert is sent to the border police and the corresponding passenger is targeted for examination on arrival. If the match is against a risk profile, a target is created. Collected and transmitted API data have to be deleted by carriers and authorities within 24 hours of transmission or arrival. However, the border authorities can retain the temporary files for longer than 24 hours if the data are needed later for the purpose of exercising the statutory functions of the border authorities or for the enforcement of laws and regulations on entry and immigration, including their provisions on the protection of public policy (*ordre public*) and national security.

3.19. Road safety related traffic offences

Legislation

Directive (EU) 2015/413 of the European Parliament and of the Council of 11 March 2015 facilitating cross-border exchange of information on road-safety-related traffic offences, OJ L 68/9

Key Provisions

Member States grant each other online access to their national Vehicle Registration Data (VRD) with a view to enforcing sanctions for certain road safety related offences committed with a vehicle which is registered in a Member State other than the Member State where the offence took place. The Member State of the offence uses the data obtained in order to establish who is personally liable for the traffic offence. The information exchange applies to:

- speeding;
- non-use of a seatbelt;
- failing to stop at a red traffic light;
- drink-driving;
- driving under the influence of drugs;
- failing to wear a safety helmet;
- use of a forbidden lane;
- illegally using a mobile telephone or any other communication device while driving.

Using the specific EUCARIS software application, Member States reciprocally allow their designated National Contact Points (NCP) access to VRD, with the power to conduct automated searches on

a) data relating to vehicles and

b) data relating to the owner or holder of the vehicle.

3.20. Entry / Exit System (EES)

Legislation

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, OJ L 327/20, 9.12.2017.

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135/27, 22.5.2019.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019.

The Regulation constitutes a development of the provisions of the Schengen *acquis.*

Denmark gave notice that it has decided to implement the above Regulations in Danish law, under Article 4 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union. That decision creates an obligation under international law between Denmark and the other Member States bound by the measures.

The United Kingdom and Ireland do not take part in the *acquis* and are therefore are not bound by the Regulation or subject to its application.

Iceland, Norway, Liechtenstein and Switzerland are bound by the *acquis* within the meaning of the respective Agreements or Protocol regarding the Schengen *acquis*.

As regards Cyprus, Bulgaria, Romania and Croatia, the provisions of the Regulation relating to SIS and VIS constitute provisions building upon, or otherwise related to, the Schengen *acquis* within the meaning of the respective Acts of Accession.

Key provisions

The Regulation[90] specifies the objectives of the EES, the categories of data to be entered into the EES, the purposes for which the data are to be used, the criteria for their entry, the authorities authorised the access to the data, further rules on data processing and the protection of personal data, as well as the technical architecture of the EES, rules concerning its operation and use, and interoperability with other information systems. EES aims at improving external border management, at preventing irregular immigration and at facilitating the management of migration flows. To that end, EES is designed to record and store the data, time and place of entry and exit of certain third-country nationals crossing the border of the Member States at which the EES is operated. Additionally, the EES may be consulted for the purposes of the prevention, detection or investigation of terrorist offences and of other serious criminal offences by national law enforcement authorities.[91]

The EES consists of a central system (EES Central System), which operates a computerised central database of biometric and alphanumeric data, a National Uniform Interface in each Member State. A secure communication channel connects the EES central system to the central Visa Information System (VIS Central System), and a secure and encrypted communication infrastructure connects the EES central system to the national uniform interface. Interoperability is established between the EES and the VIS by way of a direct communication channel between their central systems so to enable border authorities to consult the VIS from EES and visa authorities to consult the EES from VIS.

---

90 The Commission will determine the date from which EES is to start operations once the conditions set out in Article 66 of Regulation (EU) 2017/2226 are met.

91 'Terrorist offence' means an offence which corresponds or is equivalent to one of the offences referred to in Directive (EU) 2017/541; 'serious criminal offence' means an offence which corresponds or is equivalent to one of the offences referred to in Art. 2(2) of Framework Decision 2002/584/JHA on the European Arrest Warrant, if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.

The Regulation establishes strict rules concerning access to the EES. It also sets out the individuals' right of access, rectification, completion, erasure and redress, in particular the right to judicial remedy and the supervision of processing operations by public independent authorities.

The Regulation respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the EU. Without prejudice to more specific rules laid down in the Regulation for the processing of personal data, Regulation (EU) 2016/679[92] ('General Data Protection Regulation') applies to the processing of personal data in application of this Regulation unless such processing is carried out by the designated law enforcement authorities or central access points of the Member States, in which cases Directive (EU) 2016/680[93] ('Police Directive') applies.

3.21. European Travel Information and Authorisation System (ETIAS)

Legislation

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236/1, 19.9.2018.

Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS), OJ L 236/72, 19.9.2018.

---

92 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4.5.2016

93 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2019 on the protection of natural persons with regard to personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offence or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decisions 2008/977/JHA, OJ L 119/89, 4.5.2016

Regulation 2018/1240[94] specifies the objectives of ETIAS, defines its technical and organisational architecture, lays down rules concerning the operation and use of the data to be entered into the system by the applicant and rules on the issue or refusal of the travel authorisation, lays down the purposes for which the data are to be processed, identifies the authorities entitled to access the data and ensure the protection of personal data.

The Regulation constitutes a development of the provisions of the Schengen acquis. The United Kingdom and Ireland do not take part in the acquis and are therefore not bound by the Regulation or subject to its application. Iceland, Norway, Liechtenstein and Switzerland are bound by the *acquis* within the meaning of the respective Agreements or Protocol regarding the Schengen *acquis*.

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135/27, 22.5.2019.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019.

Key provisions

ETIAS provides a travel authorisation, which by nature is distinct from a visa but constitutes a condition of entry and stay in the Schengen Area, and which indicates that the applicant for a travel authorisation does not pose a security, illegal immigration or high epidemic risk in the Union.

94 The Commission will determine the date from which ETIAS is to start operations once the conditions set out in Article 88 of Regulation (EU) 2018/1240 are met.

ETIAS consists of a

- large scale information system, i.e. the ETIAS information system, which is designed, developed and technically managed by eu-LISA;
- the ETIAS Central Unit, which is part of the European Border and Coast Guard Agency;
- the ETIAS National Units, responsible for examining applications and deciding whether to issue or refuse, annul or revoke travel authorisations. To that end, the national units should cooperate with each other and with Europol for the purpose of assessing applications.

Access to personal data in ETIAS should be limited to strictly authorised personnel and in no circumstances should access be used to reach decisions based on any form of discrimination. As regards law enforcement authorities designated by the Member States, the processing of personal data stored in the ETIAS Central System should take place only in specific cases and only when it is necessary for the purposes of preventing, detecting or investigating terrorist or serious criminal offences. The designated authorities and Europol should only request access to ETIAS when they have reasonable grounds to believe that such access will provide information that will assist them in preventing, detecting or investigating a terrorist or serious criminal offence.

The Regulation respects fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union. With regard to the processing of personal data, appropriate safeguards aim therefore at keeping the interference with the right to protection of private life and to the right of protection of personal data limited to what is necessary and proportionate in a democratic society.

Regulation (EU) 2016/679 ('General Data Protection Regulation')[95] applies to the processing of personal data in application of this Regulation unless such processing is carried out by the esignated law enforcement authorities or central access points of the Member States, in which cases Directive (EU) 2016/680[96] ('Police Directive') applies.

3.22. Interoperability Legislation

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135/27, 22.5.2019.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135/85, 22.5.2019.

Key provisions

Regulation (EU) 2019/817 and Regulation (EU) 2019/818 form the 'interoperability package' and focus on personal data stored in information systems which are centralised at EU level. The Regulations aim at improving the Union's data management architecture for both border management and security. Thus, the framework of the 'interoperability package' applies to the processing of personal data in the field of either borders and visa or police and judicial cooperation, asylum and migration. Interoperability between these underlying information systems should allow them to supplement each other in order to better achieve their respective purposes.

---

95 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 4.5.2016.

96 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2019 on the protection of natural persons with regard to personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offence or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decisions 2008/977/JHA, OJ L 119/89, 4.5.2016.

The Regulations also adapt the procedures and conditions for the designated authorities and for Europol to access the EES, VIS, ETIAS and Eurodac for the purposes of prevention, detection or investigation of terrorist offences and serious crime.

The technical interoperability components cover the EES (see pt. 3.18), VIS (see pt. 3.7), ETIAS (see pt. 3.19), Eurodac (see pt. 3.8), SIS (see pt. 3.2), and ECRIS-TCN (see pt. 3.13.2). The interoperability components[97] are the:

- European search portal (ESP), understood as a single window or 'message broker', which enables the above EU instruments, Europol data and Interpol databases to be queried in parallel. Queries are limited to data related to persons or travel documents;

- shared biometric matching service (shared BMS), whose main purpose is to facilitate the identification of an individual registered in several databases by using a single technological component to match that individual's biometric data across different systems. The AFIS templates in use should be regrouped and stored in the BMS in one single location;

- common identity repository (CIR), understood as a shared container for identity data, travel documents and biometric data of persons registered in the EES, VIS, ETIAS, Eurodac and ECRIS-TCN. These data may relate to the same person but under different or incomplete identies. Increased accuracy of identification should be achieved through automated comparison and matching of the data. The CIR provides for identity checks by designated law enforcement authorities in order to support their efforts to identify a person;

- multiple identity detector (MID), which supports the functioning of the CIR.

The new data processing operations provided for by the Regulations interfere with the fundamental rights as protected by Articles 7 and 8 of the Charter of Fundamental Rights of the EU. Since the effective implementation of the EU information systems is dependent upon correct identification of the individual concerned, such interference is in line with the objectives for which each of those systems have been established, the effective management of the Union's borders, the internal security of the Union and the effective implementation of the Union's asylum and visa policies.

---

97 The Commission will determine the date from which the provisions of the Regulations related to the ESP, the shared BMS, the CIR and the MID will apply.

Regulation (EU) 2016/679 applies to the processing of personal data for the purpose of interoperability unless such processing is carried out by designated law enforcement authorities or central access points of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of serious criminal offences . In this case, Directive (EU) 2016/680 (see pt. 3.0) applies.

The supervisory authorities referred to in Regulation (EU) 2016/679 or Directive (EU) 2016/680 should monitor the lawfulness of the processing of personal data by the Member States. The European Data Protection Supervisor should monitor the activities of the Union institutions and bodies in relation to the processing of personal data.