Council of the
European Union

Brussels, 5 September 2019
(OR. en)

9364/19

DAPIX 184
ENFOPOL 252
CT 53
ENFOCUSTOM 105
CRIMORG 81
SCHENGEN 23
VISA 116
SIRIS 97
COPEN 219
ASIM 62
FRONT 190
COMIX 273
JAI 529

NOTE

From:	General Secretariat of the Council
To:	Working Party on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	6727/18
Subject:	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 current version takes, in particular, account of the Europol Regulation and of contact details. These contact details are regularly updated by the Member States and set out in the national factsheets, which are from now on 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]. A new element is the practical advisor (ADD 2) which provides a comparison of requirements for exchange of information via different channels.

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.

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.

[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 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.

In addendum, the manual is completed by

(a) a compilation of **national fact sheets** for each Member State, containing **practical details on contact points** relevant for cross-border information exchange, and

(b) the requirements for information exchange in view of the different channels in use (Interpol/ Europol/ SIRENE/ Liaison Officers/PCCC) and more practical advice set out in a user-friendly way.

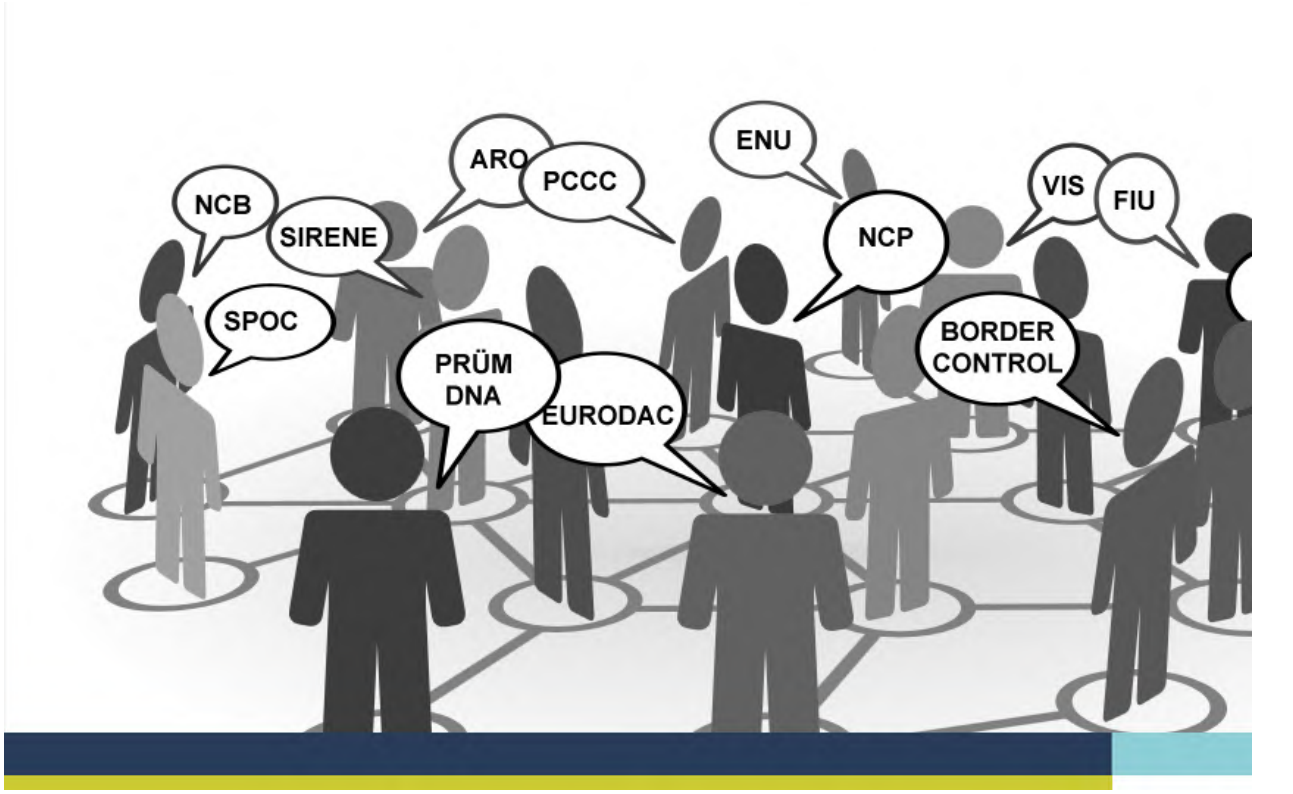
4. Way forward

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, the Presidency submits the current and updated version to delegations and invites them to disseminate it appropriately in the light of their needs.

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[2] 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**

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.

[2] 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).

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 1 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 IV - 'Practical Advisor for Law Enforcement Information Exchange

Addendum 2 to this note, the Practical Advisor, provides in a user-friendly way a comparison of the requirements for information exchange in view of different channels (Interpol/ Europol/ SIRENE/ Liaison Officers/PCCC). It provides furthermore practical information and advices related to instruments for law enforcement cooperation which could be beneficial not only for SPOC officers but also for other national law enforcement bodies.

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 Council Decision 2007/533/JHA, OJ L 205/63, 7.8.2007 Regulation (EC) No 1986/2006 OJ L 381/1, 28.12.2006 Regulation (EC) 1987/2006 OJ L 381/4, 28.12.2006	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

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 Council Decision 2007/533/JHA, OJ L 205/63, 7.8.2007 Regulation (EC) No 1986/2006 OJ L 381/1, 28.12.2006 Regulation (EC) 1987/2006 OJ L 381/4, 28.12.2006	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	

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

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[3]

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.

Principle of Availability - SFD

Exchange of law enforcement[4] information and intelligence of cross-border relevance should comply with the conditions which derive from the 'principle of availability' implemented by the 'Swedish Framework Decision' (SFD). This means that:

- a law enforcement officer in one Member State who needs information in order to carry out his duties can obtain it from another Member State and that
- the law enforcement authorities in the Member State that holds this information will make it available for the declared purpose, taking account of the needs of investigations pending in that Member State, and that

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

[4] 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), if it is punishable under national law by a custodial sentence or detention order for a maximum period of at least three years.

- once police information is available in a Member State, it shall be shared across borders under the same conditions which govern information sharing at national level, meaning that the rules applied in a cross border case are not stricter than those applying to data exchanges at national level ('principle of equivalent access').

Single Point of Contact (SPOC)

The combination of the strict requirements of the Swedish Framework Decision and the existence of different national strategies to manage the various information exchange initiatives requires a more simple and uniform approach at the Member State level in order to ensure that all requests for information between law enforcement agencies in the EU are dealt with effectively and efficiently.

The Council Conclusions on the European Information Exchange Model (EIXM)[5], adopted in June 2013, recognised the potential of a single point of contact for information exchange within each Member State to help streamline the process in an increasingly complex legal and operational landscape.

The policy of effecting as much information exchange as possible through a single point of contact has been implemented by nearly all Member States although the understanding of what defines a SPOC seems to vary among the Member States. The SPOC guidelines[6] indicate how SPOCs can be structured to maximise the use of resources, avoid overlaps and make cooperation with other Member States more efficient, expedient and transparent.

From these guidelines, Member States should select the solution appropriate for their situation in view of the common and agreed aim of enhancing international cooperation, and consider appropriate ways of informing other Member States about the solution selected with a view to the exchange of best practices.

---

5 Council Conclusions following the Commission Communication on the European Information Exchange Model (EIXM), 9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146

6 'Draft Guidelines for a Single Point of Contact (SPOC) for international law enforcement information exchange', 10492/14 DAPIX 75 ENFOPOL 157 and 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1

The SPOC ideally:

- has access to the broadest range of relevant national, European and international law enforcement databases in order to expeditiously manage direct information exchange between the national competent authorities;

- houses the national SIRENE, Europol and Interpol units;

- houses the contact point for liaison officers, the contact points designated pursuant to the SFD and the 'Prüm Decisions', and, if any, the contact points for regional and bilateral offices;

- is set up in a secure working environment and sufficiently and adequately staffed, including interpretation or translation capacities, to operate on a 24/7 basis. As far as possible, all staff should be trained and equipped/mandated to deal with all kinds of tasks within the SPOC. Where this is not possible, it should be ensured that all tasks can be dealt with through on-call duty officers 24/7;

- is a multi-agency organisation, composed of staff coming from/belonging to different services and/or Ministries including criminal police, border guards, customs and judicial authorities.

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 *acquis*[7] 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[8], an alert being a set of data enabling authorities to identify persons or objects with a view to taking appropriate action.

'Supplementary information' is defined as information not stored in SIS II, but connected to SIS II alerts, which is to be exchanged, bilaterally or multilaterally, by means of forms:

(i) in order to allow Member States to consult or inform each other when entering an alert;

(ii) following a hit in order to allow the appropriate action to be taken;

(iii) when the required action cannot be taken;

(iv) when dealing with the quality of SIS II data;

(v) when dealing with the compatibility and priority of alerts;

(vi) when dealing with rights of access.

---

7 See the Convention Implementing the Schengen Agreement, OJ L 239, 22.9.2000.

8 See 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.

Information is to be exchanged in accordance with the provisions of the SIRENE Manual[9] and using the Communication Infrastructure. [10] SIS II[11] has enhanced functionalities compared to its predecessor, such as the possibility to enter fingerprints and photographs, new types of objects (stolen aircraft, boats, containers, means of payment) as well as the possibility for the owner of the alert to link different alerts. SIS II contains copies of European Arrest Warrants (EAW) attached directly to alerts on the persons concerned.

SIRENE bureaux facilitate co-operation on police matters and may also have a role in information exchange outside the scope of SIS II pursuant to provisions previously covered by Articles 39 and 46 of the CISA which have been replaced by **the 'Swedish Framework Decision'.** According to Article 12 (1) of the 'Swedish Framework Decision' the provisions of Article 39(1), (2) and (3) and of Article 46 of the Convention Implementing the Schengen Agreement (CISA), in so far as they relate to exchange of information and intelligence for the purpose of conducting investigations or criminal intelligence operations as provided for by the Framework Decision, are replaced by the provisions of the Framework Decision.

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.

---

9 Commission Implementing Decision of 26 February 2013 on the Sirene Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2013) 1043**),** OJ 71/1, 14.3.2013.

10 Due to the closure of the SISnet mail network, SIRENE Bureaux may now use the sTESTA mail service. Other information exchanges may take place over the sTESTA network, SIENA or I-24/7 communication channels.

11 Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA; 15810/16 SIRIS 175 COMIX 860

Europol[12] 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.

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.

[12] 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)

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'[13] 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[14]. 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.

---

13 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.

14 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[15]

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)[16]

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.

---

15 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).

16 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[17] contained in the appendix to the Football Handbook.

1.6.1. The Football Handbook[18]

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. 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).

---

17 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.

18 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.

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 in accordance with Council Decision 2006/960/JHA ('Swedish Framework Decision').

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.

1.8. 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[19] 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.

[19] '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.*

1.9. 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.[20]

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[21], 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[22] 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.

---

20 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.

21 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.

22 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.

1.10. Money Laundering - Cooperation between Financial Intelligence Units (FIU)[23] [24]

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.

---

23 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.

24 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 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.

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.

1.11. Naples II Convention[25]

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.

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.

[25] 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.

1.12. Passenger Information Unit (PIU)

In the framework of Directive 2016/681[26], 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[27] 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.

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.

---

[26] 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.

[27] 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 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.[28]

[28] 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.

1.13. EES national access points

The Entry/Exit System[29] (EES) aims primarily at improving the Union's external border management and is used to that effect by border, immigration and visa authorities[30]. 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.

---

29 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.

30 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.[31]

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.

1.14. ETIAS National Unit[32]

The European Travel Information and Authorisation System (ETIAS) supports[33] 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.

---

31 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.

32 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.

33 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.

1.15. Interoperability

The main objective of the 'interoperability package'[34] 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.[35]

(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.

---

[34] 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.

[35] 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.

1.16. Choosing the channel – Commonly used criteria

In a Member State, the SPOC[36] 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:

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

- SIRENE via the contact points of each Schengen State for SIS
- EUROPOL via the Europol National Units / Europol Liaison Officers
- 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:

- 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)[37]

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. [38]

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, an alert being a set of data enabling authorities to identify persons or objects with a view to taking appropriate action:

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;

---

[37] 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.

[38] 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*.

– 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.

2.2. EIS – The Europol Information System[39]

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 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;

---

[39] 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)

(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, including data exchange in accordance with the 'Swedish Framework Decision'.

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 UMF PERSON entity 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.[40]

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.

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

2.5. ECRIS[41]

The IT-based European Criminal Records Information System (ECRIS) [42] 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.

---

41 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.

42 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[43]

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[44], 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.

---

43 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

44 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)[45]

The Visa Information System (VIS) is principally an immigration control system. It is a tool used to facilitate consultation at the level of consulates and border control through electronic verification and exchange of visa data between Member States. As such, it targets visa required foreign nationals. Member States' designated authorities (i.e. consular posts, border checkpoints, police and immigration authorities)[46] and Europol[47], within the framework of its tasks, are allowed to consult the VIS[48] for the purposes of the prevention, detection and investigation of:

- terrorist offences, i.e. those offences under national law which correspond or are equivalent to the offences in Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June on combating terrorism, and of

- serious criminal offences, i.e. the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA ('European Arrest Warrant').

---

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

46 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

47 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.

48 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.

In accordance with the SFD, information contained in the VIS can be provided to UK and IE by the competent authorities of the Member States whose designated authorities have access to the VIS, and information held in the national visa registers of UK and IE can be transmitted to the competent law enforcement authorities of the other Member States.

The VIS is based on a centralised architecture and a common platform with SIS II. VIS data is processed in two steps. In the first step, data comprises alphanumeric data and photographs. In the second step, biometric data and scanned documents are processed and entered in the VIS. The VIS includes data on visa applications, photographs, fingerprints, related decisions of visa authorities and links between related applications. The VIS uses a biometric matching system to ensure reliable fingerprint comparisons for the purpose of either:

- verification, i.e. a check whether fingerprints scanned at the border crossing point correspond to those associated with the biometric record attached to the visa, or

- identification, i.e. a comparison of the fingerprints taken at the border crossing post with the contents of the entire database.

Technically speaking, the VIS consists of three levels, namely the central, national and local level, the latter including consular posts, border crossing points, and immigration and police authorities. 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 area of justice and home affairs. The upgraded VIS is not expected to be operational before the end of 2021.

2.7. Eurodac[49] [50]

The European Automated Fingerprint Identification System (Eurodac) originally assists in determining the Member State responsible for examining applications for asylum lodged in one of the Member States, and otherwise in facilitating the application of the Dublin Convention. Access to Eurodac for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences is given only in well-defined cases.

The Eurodac Regulation 603/2013 lays down rules on the transmission of fingerprint data to the Central Unit, the recording of this data and other relevant data in the relevant central database, storage of the data, its comparison with other fingerprint data, transmission of the results of this comparison and the blocking and erasure of recorded data.

The Eurodac system architecture consists of (a) a computerised central fingerprint database ('Central System') composed of a Central Unit and a Business Continuity Plan and System, and (b) a communication infrastructure between the Central System and Member States, which provides an encrypted virtual network dedicated to Eurodac data ('Communication Infrastructure').

Each Member State has a single National Access Point.

'eu-LISA, established by Regulation (EU) 1077/2011[51], is responsible for the operational management of Eurodac, and shall ensure, in cooperation with the Member States, that at all times the best available and most secure technology and techniques, subject to a cost-benefit analysis, are used for the Central System.

---

[49] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316/1, 15.12.2000.

[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).

[51] Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286/1, 1.11.2011.

Any Member State may transmit fingerprints to the Central Unit with a view to checking whether an alien of at least 14 years of age found illegally present in its territory has already lodged an application for asylum in another Member State. The Central Unit compares these fingerprints with fingerprint data transmitted by other Member States and already stored in the central database. The Unit informs the Member State that has transmitted the data as to whether there is a 'hit', that is the result of the comparison between fingerprints recorded and transmitted. This Member State checks the result and proceeds to the final identification in cooperation with the Member States concerned.

Member States have to ensure the lawfulness, accuracy and security of Eurodac data. Any person who, or Member State which, has suffered damage as a result of non-compliance with Eurodac provisions is entitled to receive compensation from the Member State responsible for the damage suffered.

Regulation (EU) No 603/2013 provides for access to Eurodac data by Member States' designated authorities and by Europol for law enforcement purposes. According to the Regulation, designated authorities may submit a reasoned electronic request for the comparison of fingerprint data with the data stored in the Central System only if comparisons with the following databases did not lead to the establishment of the identity of the data subject:

– National fingerprint databases.

– The automated fingerprinting identification systems (AFIS) of all other Member States under Decision 2008/615/JHA ('Prüm Decisions') where comparisons are technically available, unless there are reasonable grounds to believe that a comparison with such systems would not lead to the establishment of the identity of the data subject. Such reasonable grounds shall be included in the reasoned electronic request for comparison with Eurodac data sent by the designated authority to the verifying authority.

– The Visa Information System (VIS), provided that the conditions for such a comparison laid down in Decision 2008/633/JHA are met.

The following cumulative conditions must also be met:

a) The comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, which means that there is an overriding public security concern which makes the searching of the database proportionate.

b) The comparison is necessary in a specific case (i.e. systematic comparisons shall not be carried out).

c) There are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question. Such reasonable grounds exist in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls in a category covered by Regulation (EU) No 603/2013.

2.8. CIS – Customs Information System[52]

The Customs Information System complements the Naples II Convention[53]. 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.

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 [54]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.

---

52 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.

53 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.

54 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.

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.

2.9. False and Authentic Documents Online - FADO[55]

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

[55] 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.

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.

2.10. 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[56] 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.

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

2.11. Entry / Exit System (EES)

The Entry / Exit System[57] (EES) aims primarily at improving the Union's external border management[58]. It 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.

Additionally, the EES may be consulted, only under the conditions laid down in the Regulation, by national law enforcement authorities for the purposes of prevention, detection or investigation of terrorist offences and of other serious criminal offences.

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.

The EES consists of

- a central system (EES Central System), which operates a computerised central database of biometric (fingerprint data and facial images) and alphanumeric data,
- a national uniform interface in each Member State,
- a secure and encrypted communication infrastructure, which connects the EES central system to the national uniform interface,
- a secure communication channel, which connects the EES central system to the Visa Information System (VIS) central system for consultation purposes.

---

[57] 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

[58] 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.

The regulation specifies which national authorities are entitled to have access to the EES in order to enter, amend, erase or consult data for the specific purposes of the EES and to the extent necessary for the performance of their tasks. Any processing of EES data should be proportionate to the objectives pursued and necessary for the performance of the task of the competent authorities.

The conditions of access to the EES for national law enforcement authorities are such as to allow these authorities to tackle the cases of suspects using multiple identities. The specific use of EES stored biometric data is justified, despite its impact on the privacy of the traveller, to identify travellers without traveller documents or any other identification. However, such data may also be used to construct evidence by tracking the travel routes of a person suspected of having committed a crime, or of a victim of crime.

Access to EES data for law enforcement purposes constitutes an interference with the fundamental rights to respect for private life and to protection of personal data of persons whose data are processed in the EES. Such processing is governed by the provisions of Directive (EU) 2016/680 ('Police Directive')[59] .

In pursuing their tasks, national law enforcement authorities may compare a dactyloscopic trace found at a crime scene ('latent fingerprints') with fingerprint data stored in the EES where there are reasonable grounds for believing that the perpetrator or victim is stored in the EES. However, law enforcement access to the EES for identifying unknown suspects, perpetrators or victims of terrorist offences or other serious criminal offences is subject to the condition that searches in the national databases have been carried out and the fingerprint search within Council Decision 2008/615/JHA[60] ('Prüm Decision') has been fully conducted, or the search has not been fully conducted within two days of being launched.

---

[59] 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

[60] 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, 6.5.2008

Similar to the procedures and conditions for access by national law enforcement authorities, EES data are also available to Europol, within its tasks and subject to the conditions and limitations set out in the Regulation. Europol processes information obtained from a consultation of EES data subject to the authorisation of the Member States of origin. That authorisation shall be obtained via the Europol national unit of that Member State. The European Data protection Supervisor should monitor the processing of data by Europol and ensure full compliance with applicable data protection rules.

2.12. European Travel Information and Authorisation System (ETIAS)[61]

Information exchange in the field of border management, law enforcement and counter-terrorism will be supported by ETIAS[62]. The system aims to determine the eligibility of visa-exempt third-country nationals prior to their travel to the Schengen Area and their arrival at external border crossing points. ETIAS provides a travel authorisation, which by nature is distinct from a visa but constitutes a condition of entry and stay, and which indicates that the applicant does not pose a security, illegal immigration or high epidemic risk. Issued travel authorisations should be annulled or revoked as soon as it becomes obvious that the conditions for issuing them were not or are not longer 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;

---

61 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

62 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.

- 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.

Personal data provided by the applicant are only processed by ETIAS for the purposes of assessing whether the entry of the applicant into the Union could pose a security, illegal immigration or high epidemic risk in the Union. For the assessment of risks, personal data provided should be compared with the data present in a record, file or alert registered in an EU information system or database (the ETIAS Central System, SIS, the Visa Information System (VIS), the Entry/Exit System (EES) or Eurodac), in Europol data or in the Interpol databases (the Interpol Stolen and Lost Travel Documents database (SLTD) or the Interpol Travel Documents Associated with Notices (TDAWN). The personal data should also be compared against the ETIAS watchlist and against specific risk indicators.

The comparison takes place by automated means. Should a "hit" occur, that is a correspondence between personal data in the application and the specific risk indicators or the personal data either in a record file or alert in the above information systems or the watchlist, the application should be processed manually by the National Unit of the Member State responsible. Such assessment should lead to the decision to issue the travel authorisation or not to do so.

In order to reach the overall objectives of ETIAS, the processing of significant amounts of personal data is involved. The Regulation respects fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union. 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. For the same reason, the criteria used for defining the specific risk indicators should in no circumstances be based on sensitive personal data.[63]

[63] See 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.

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, 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.

2.13. 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	
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, 7.6.20199	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[64] 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

[64] 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 o 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[65] 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

[65] 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[66]

Directive (EU) 2016/680, which repeals Council Framework Decision 2008/977/JHA[67], lays down the specific rules relating to

- the protection of natural persons, whatever their nationality or place of residence, with regard to the processing, whether by automated means or otherwise, of personal data by the police or other law enforcement authorities within the remit of their activities, and
- the exchange of personal data within the Union by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

It aims at ensuring the same level of protection for natural persons by establishing legally enforceable rights throughout the Union and at preventing divergence practices which hamper the exchange of personal data between the competent authorities.

Member States shall transpose the directive by 6 May 2018. However, in cases where this involves disproportionate effort, they may exceptionally provide that they will implement by 6 May 2023 the relevant monitoring provisions for operations in automated processing systems set up before 6 May 2016.

---

66 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.

67 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matter, OJ L 350/60, 30.12.2008. The Framework Decision is repealed with effect from 6 May 2018.

The term 'competent authorities' covers public authorities such as the judicial authorities, the police or other law enforcement authorities, as well as any other body or entity entrusted by the law of a Member State to exercise public authority and public powers for the purposes of this directive. The activities of law enforcement authorities focus mainly on the prevention, investigation, detection or prosecution of criminal offences. Such activities can also include police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on them, where necessary, to safeguard against and prevent threats to public security and to the fundamental interests of the society which may lead to a criminal offence.

The processing of personal data for purposes outside the scope of the activities mentioned above and with which Member States may additionally entrust law enforcement authorities, and the processing of personal data, insofar as it is within the scope of Union law, is governed by Regulation (EU) 2016/679[68]. Furthermore, Directive (EU) 2016/680 does not cover the processing of personal data with regard to activities concerning national security, the activities of agencies or units dealing with national security issues or the processing of personal data by the Member States when carrying out activities with regard to the common foreign and security policy[69].

For the purposes of the Data Protection Directive:

- **'personal data'** means any information relating to a natural person ('data subject') identified or identifiable, directly or indirectly, in particular by reference to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

  Member States shall provide that the competent authorities processing personal data, where applicable and as far as possible, will make a clear distinction between personal data of different categories of data subjects, such as (a) suspects, (b) convicts, (c) victims and (d) other parties to a criminal offence, such as witnesses.

---

68 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

69 Chapter 2 of Title V of the Treaty on European Union (TEU)

- **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data must be processed lawfully and fairly, and only for specific purposes laid down by law. In order to be lawful, such processing should be necessary for the performance of a task carried out by a competent authority for the abovementioned law enforcement purposes. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamentals Freedoms. Personal data must be adequate and relevant for the purposes for which they are processed.

The processing of particularly sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the sole purpose of identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only under well defined and restrictive conditions.

The establishment of national supervisory authorities that are able to exercise their functions with complete independence is an essential component of the protection of natural persons with regard to the processing of their data. The supervisory authorities should monitor the application of the provisions adopted pursuant to the directive and should contribute to their consistent application throughout the Union. The protection of rights and freedoms of data subjects as well as the responsibility and liability of national competent authorities and processors, also in relation to monitoring by supervisory authorities and any measures taken by such authorities, requires a clear attribution of responsibilities.

Moving personal data across borders may jeopardise the ability of natural persons to protect themselves legally from unlawful use or disclosure of those data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers and inconsistent legal regimes. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities in order to help them exchange information with their foreign counterparts.

3.2. The 'Swedish Framework Decision' (SFD)[70]

As a development of the Schengen *Acquis,* Council Framework Decision 2006/960/JHA ('Swedish Framework Decision' - SFD) sets out, in particular, the rules regarding time limits and standard forms for cross-border information exchange[71], on prior request or spontaneously, between the designated competent law enforcement authorities of the Member States for the purpose of:

- preventing, detecting and investigating offences or criminal activities which correspond to or are equivalent to those referred to in the European arrest warrant[72], or
- preventing an immediate and serious threat to public security.

The designated authorities are obliged to reply within at most eight hours in urgent cases, as long as the requested information or intelligence is directly accessible to law enforcement authorities. Information may not be provided if:

- national security is at stake,
- current investigations may be jeopardised,

---

70 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.

71 See infra Figure 1.

72 8216/2/08 REV2 Final version of the European handbook on how to issue a European Arrest Warrant. Article 2 of Council Framework Decision 2002/584/JHA on the European Arrest Warrant sets out the scope of the EAW.

- the request pertains to an offence punishable by a term of imprisonment of one year or less under the law of the requested Member State,

- the competent judicial authority withholds access to the information.

The terms 'information and/or intelligence' cover the following two categories:

– any type of information or data which is held by law enforcement authorities

– any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures

The content of these categories depends on national legislation. The type of information available from each Member State is set out in the national sheets attached to this manual.

Data is to be shared with Europol insofar as the information or intelligence exchanged refers to an offence or criminal activity within the Europol mandate. Information and intelligence will be processed in accordance with the relevant Europol handling codes. SIENA, (Europol's Secure Information Exchange Network Application) supports the exchange of information in accordance with the 'Swedish Framework Decision'.

Member States ensure that conditions for cross-border information exchange are not stricter than those applicable for an internal case. The competent law enforcement authorities are, in particular, not obliged to ask for judicial agreement or authorisation prior to cross-border information exchange, if the information sought is available at national level without such agreement or authorisation. If, however, judicial authorisation is required, the judicial authority shall, when issuing its decision, is required to apply the same rules in the cross-border case as in a purely internal case. Information requiring judicial authorisation is indicated in the national fact sheets.

Since the standard request form has been found too cumbersome by practitioners, a non-compulsory request form for information and intelligence[73] has been developed. When it is not feasible to use this simplified form, the use of a different form or unstructured free-text is preferred.

[73] See infra Figure 2.

However, these requests shall in all cases comply with the requirements of Article 5 of the Swedish Framework Decision, and contain at least the following mandatory items:

- administrative information, i.e. requesting Member State, requesting authority, date, reference number(s), requested Member State(s)
- whether urgency is requested, and, if so, what the reasons are
- description of the requested information or intelligence
- identity/identities (as far as known) of person(s) or object(s) who are the main subject(s) of the criminal investigation or criminal intelligence operation underlying the request for information or intelligence (e.g. description of the offence(s), circumstances in which the offence(s) was (were) committed etc.)
- purpose for which the information and intelligence is sought
- connection between the purpose and the person who is the subject of the information and intelligence
- reasons for believing that the information or intelligence is in the requested Member State
- any restrictions on the use of information contained in the request ('handling codes')

The requesting Member State may choose between any of the existing channels for international law enforcement communication (SIRENE, EUROPOL, INTERPOL, bilateral contact points). The replying Member State normally uses the same channel as used for the request. If, however, the requested Member State replies, for legitimate reasons, through another channel, the requesting authority is informed of this change. The language used for the request and supply of information shall be the one applicable for the channel used.

An overview of the **bilateral or other agreements maintained** is annexed to this manual.

Figure 1

ANNEX A

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

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

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

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

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

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

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

❑ No
❑ Yes

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

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

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

It is likely to be given within:

❑ 1 day ❑ 2 days ❑ 3 days
❑ .... weeks
❑ 1 month

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

REFUSAL — The information or intelligence:
❑ could not be provided and requested at national level; or
❑ cannot be provided, for one or more of the following reasons:

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

❑ the competent judicial authority has not authorised the access and exchange of the information or intelligence

❑ the requested information or intelligence has previously been obtained by means of coercive measures and its provision is not permitted under the national law

❑ the information or intelligence is not held

- by law enforcement authorities; or
- by public authorities or by private entities in a way which makes it available to law enforcement authorities without the taking of coercive measures

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

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

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

❑ E — The requested information or intelligence is not available

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

ANNEX B

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

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

I — Administrative information

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

Previous requests				
❑ This is the first request on this case				
❑ This request follows previous requests in the same case				
Previous request(s)			Answer(s)	
	Date	Reference number (in the requesting Member State)	Date	Reference number (in the requested Member State)
1.				
2.				
3.				
4.				

If the request is sent to more than one authority in the requested Member State, please specify each of the channels used:	
❑ ENU/Europol Liaison Officer	❑ For information ❑ For execution
❑ Interpol NCB	❑ For information ❑ For execution
❑ Sirene	❑ For information ❑ For execution
❑ Liaison Officer	❑ For information ❑ For execution
❑ Other (please specify):	❑ For information ❑ For execution
If the same request is sent to other Member States, please specify the other Member States and the channel used (optional)	

II — Time limits

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

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

and

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

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

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

B — Other cases: time limit: 14 days

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

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

Nature of the offence(s)

A — Application of Article 4(1) or 4(3) of the Framework Decision 2006/960/JHA

❑ A.1. The offence is punishable by a maximum term of imprisonment of at least three years in the requesting Member State
AND
A.2. The offence is one (or more) of the following:

- ❑ Participation in a criminal organisation
- ❑ Terrorism
- ❑ Trafficking in human beings
- ❑ Sexual exploitation of children and child pornography
- ❑ Illicit trafficking in narcotic drugs and psychotropic substances
- ❑ Illicit trafficking in weapons, munitions and explosives
- ❑ Corruption
- ❑ Fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests
- ❑ Organised or armed robbery
- ❑ Illicit trafficking in cultural goods, including antiques and works of art
- ❑ Swindling
- ❑ Racketeering and extortion
- ❑ Counterfeiting and piracy of products
- ❑ Forgery of administrative documents and trafficking therein
- ❑ Forgery of means of payment
- ❑ Illicit trafficking in hormonal substances and other growth promoters
- ❑ Laundering of the proceeds of crime
- ❑ Counterfeiting of currency, including the euro
- ❑ Computer-related crime
- ❑ Environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties
- ❑ Facilitation of unauthorised entry and residence
- ❑ Murder, grievous bodily injury
- ❑ Illicit trade in human organs and tissue
- ❑ Kidnapping, illegal restraint and hostage-taking
- ❑ Racism and xenophobia
- ❑ Illicit trafficking in nuclear or radioactive materials
- ❑ Trafficking in stolen vehicles
- ❑ Rape
- ❑ Arson
- ❑ Crimes within the jurisdiction of the International Criminal Court
- ❑ Unlawful seizure of aircraft/ships
- ❑ Sabotage

→ The offence therefore falls under Article 2(2) of Framework Decision 2002/584/JHA→ Article 4(1) (urgent cases) and 4(3) (non urgent cases) of Framework Decision 2006/960/JHA are therefore applicable as regards time limits for responding to this request

Or

❑ B — The offence(s) is(are) not covered under A.
In this case, description of the offence(s):

Purpose for which the information or intelligence is requested

Connection between the purpose for which the information or intelligence is requested and the person who is the subject of the information or intelligence

Identity(ies) (as far as known) of the person(s) being the main subject(s) of the criminal investigation or criminal intelligence operation underlying the request for information or intelligence

Reasons for believing that the information or intelligence is in the requested Member State

Restrictions on the use of information contained in this request for purposes other than those for which it has been supplied or for preventing an immediate and serious threat to public security

❑ use granted
❑ use granted, but do not mention the information provider
❑ do not use without authorisation of the information provider
❑ do not use

Figure 2

REQUEST FOR INFORMATION AND INTELLIGENCE

Under Council Framework Decision 2006/960/JHA

I – Administrative Information

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

Requested Member State(s):		
Channel		
☐ENU/Europol Liaison Officer	☐For information	☐For execution
☐Interpol NCB	☐For information	☐For execution
☐SIRENE	☐For information	☐For execution
☐Liaison Officer	☐For information	☐For execution
☐Other (please specify):	☐For information	☐For execution

II - Urgency

Urgency requested	☐ Yes ☐ No
Reasons for urgency (e.g.: suspects are being held in custody, the case has to go to court before a specific date): Application of Article	
Offence falls under Article 2(2) Framework Decision 2002/584/JHA on the European Arrest Warrant	☐ Yes ☐ No

III – Purpose

Type of crime(s) or criminal activity/activities being investigated
Description of: - circumstances in which the offence(s) was (were) committed (e.g.: the time, place and degree of participation in the offence(s) by the person who is the subject of the request for information or intelligence) - reasons for believing that the information or intelligence is in the requested Member State, - connection between the purpose for which the information or intelligence is requested and the person who is the subject of the information or intelligence
☐ request to use the information as evidence if possible under national legislation *(optional)*

IV – Type of information

Identity/identities (as far as known) of the person(s) or object(s)	
Person	Object(s)
Family name: Name at birth: First name: Date of Birth Place of Birth Gender: ☐male ☐female ☐unknown Nationality: Additional Information:	Weapon serial number: Document number: Other identification number or name: Vehicle registration number: Vehicle serial number (VIN): Type of documents: Contact details of company (tel. number, e-mail, address, www…): Additional Information:

Information or intelligence requested		
Person	Vehicle	Others
☐ verification of identity ☐ screening in databases ☐ finding the address/place of stay	☐ completion of identification data ☐ identification of owner ☐ identification of driver ☐ screening in databases	☐ identification of company ☐ screening of company in databases ☐ screening of documents in databases ☐ identification of phone/fax number ☐ identification of owner of the e-mail address ☐ screening of address ☐ screening of weapons ☐ weapons trading route
Others:		

V - Handling Codes

Restrictions on the use of information contained in this request for purposes other than those for which it has been supplied or to prevent an immediate and serious threat to public security
☐ for police purposes only, not for use in judicial proceedings ☐ contact the information provider prior to any use

3.3. Schengen - 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)[74] 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 two separate instruments, that is a Regulation with regard to the application of SIS at borders and a Council Decision with regard to police cooperation, does not affect the fact that the SIS constitutes one single information system.

---

[74] 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) 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.[75]

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.

[75] 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.

- 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[76] 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[77] and Croatia[78] 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.

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.

---

76 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.

77 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.

78 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.

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.

3.4. 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. Interpol

Legislation

Interpol Constitution[79]

Rules governing the processing of information[80]

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.

---

79 http://www.interpol.int/en/About-INTERPOL/Legal-materials/The-Constitution

80 http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts

3.6. Liaison officers

Legislation

Convention implementing the Schengen Agreement of 19 June 1990 (CISA)[81], 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[82]

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[83]

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:

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

---

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

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

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

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'[84] 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[85].

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.

---

84 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.

85 OJ C 314/4, 22.12.2007.

3.7. 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.[86]

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).

3.8. 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.[87]

---

[86] 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.

[87] 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.

3.9. 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[88] or of other serious criminal offences[89].

3.10. 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.

---

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

89 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).

3.10.1. Customs Information System - CIS[90]

The Customs Information System complements the Naples II Convention[91]. 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[92] 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.

3.11. 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.

---

90 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.

91 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.

92 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.

Key Provisions

Following the adoption of Council Decision 2007/845/JHA[93], 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[94] 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.

---

93 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.

94 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.

3.12. 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.

3.13. 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.

3.14. 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.

3.14.1. 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[95] 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.

[95] 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.

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.

3.15. 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.[96]

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.

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

3.16. 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[97] 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.

---

[97] 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.

3.17. 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, an alert is sent to the border police and the corresponding passenger is targeted for examination on arrival.

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.

3.18. 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.

3.19. 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[98] 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.[99]

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.

---

98 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.

99 '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[100] ('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[101] ('Police Directive') applies.

3.20. 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.

---

100 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

101 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[102] 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.

ETIAS consists of a

- large scale information system, i.e. the ETIAS information system, which is designed, developed and technically managed by eu-LISA;

[102] 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.

- 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')[103] 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[104] ('Police Directive') applies.

---

[103] 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.

[104] 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.

3.21. 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.

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[105] 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;

[105] 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.

- 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.

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.