Deloitte.

European Commission

Directorate-General
Migration and Home Affairs

Study on the implementation of the European Information Exchange Model (EIXM) for strengthening law enforcement cooperation

Final Report

26 January 2015

Deloitte

Berkenlaan 8C - 1831 Diegem - Belgium

Table of contents

Executive summary *5*

1 Introduction *8*

2 Scope and methodology of the study *9*

2.1 Scope of the study **9**

2.2 Our methodology **10**

3 Context *11*

3.1 EIXM – the rationale **11**

3.2 EIXM – the legal and policy underpinning **13**

3.2.1 The Treaty provisions 13

3.2.2 Policy frameworks for the exchange of law enforcement information 14

3.2.3 Relevant provisions in the Charter of Fundamental Rights and data protection legislation 18

3.3 EIXM – the legal instruments **20**

3.3.1 The Swedish Framework Decision 20

3.3.2 The Prüm Decisions 21

3.4 EIXM – the processes and practical aspects of information exchange **21**

4 The implementation of the European Information Exchange Model (EIXM) *26*

4.1 Implementation of the legal instruments **26**

4.1.1 Implementation and operational compliance with the Swedish Framework Decision 26

4.1.2 Implementation and operational compliance with the Prüm Decisions 39

4.2 Processes and practical aspects of information exchange **45**

4.2.1 The Single Points of Contact (SPOCs) 45

4.2.2 The channels used for information exchange 54

4.2.3 The use of instruments to exchange data from national police records 66

4.2.4 Technical developments beyond UMF II 71

4.3 Horizontal challenges of EIXM **74**

4.3.1 Training measures 74

4.3.2 Further general considerations 87

Annexes *93*

Annex 1: Analytical Framework **93**

Annex 2: Interview guides **98**

Annex 3: Glossary of terms **105**

List of figures

Figure 1: Work plan of the study 10
Figure 2: The different layers of a SPOC 46

List of tables

Table 1: Instruments of information management currently in place 16
Table 2: Main channels for the cross-border exchange of law enforcement information 22
Table 3: Evolution of Prüm implementation (2012-2014) 40
Table 4: Application of the SPOC Guidelines' criteria in the Member States 48

Acknowledgements

This assignment was conducted by a team, from Deloitte Belgium and Deloitte Germany, headed by Richard Doherty with the support of Benoît Vandresse, Éva Kamarás, Anna Siede, and external experts Jan Segerberg, prof. Paul de Hert, and prof. Valsamis Mitsilegas.

The production of this report would not have been possible without the efforts of the stakeholders interviewed or involved in the study's expert panel and the input from respondents to our web-based survey. The authors would like to express their gratitude to all of them.

Finally, the study team would like to thank the Commission officials involved for their providing information and feedback during the course of the assignment.

DISCLAIMER

By the European Commission, Directorate-General Migration and Home Affairs.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Executive summary

Smooth and secure cross-border information exchanges between law enforcement authorities are essential in order to ensure a high level of security in the EU and tackle serious and organised crime, as well as other offences that require cross-border collaboration. In order to ensure timely access to accurate and up-to-date data for law enforcement authorities, a considerable number of EU instruments and systems have been put in place in recent years, which are also supplemented by international and bilateral arrangements.

The purpose of the study was to provide a follow up to the Commission's 2012 Communication on the European Information Exchange Model (EIXM Communication), to survey and assess activities carried out in Member States in this context as well as point to possible ways of further improvement.

The conclusions of the **EIXM** Communication (in particular the fact that no new instruments are needed but rather that existing instruments need consolidating), are appreciated by the stakeholders consulted. However, the EIXM model focused on stocktaking and did not provide an overall vision in the area of information exchange. Hence there seems to be a need for more EU level overall governance and guidance in the area of police information exchange. It is noted that the increased competences of the Commission, as of December 2014, as stipulated by the Lisbon Treaty, present an important opportunity in this regard.

While the progress made in the past few years is very positive, progress with and a common understanding of the SPOC concept and the choice of channel are hindered by the lack of binding rules in these areas. Although there is funding and support at EU level, there seems to be a lack of prioritisation that in some cases hinders the implementation of EU instruments.

The delays in the implementation of Prüm and the difficulties with the application of the SFD create a situation in which progress is further slowed. These factors seem to be decreasing motivation in some Member States to put effort into the implementation and application of EU instruments, if they see that their counterparts are not doing the same.

At the same time, information exchange has increased, but the allocation of resources in Member States working in the area of information exchange has not followed this increase. Furthermore, differences in national legal and administrative systems are in general obstacles to achieving better information exchange.

As a fundamental issue, there is a lack of awareness among police corps on the availability and potential of information exchange, which also is related to the fact that existing training programmes do not fully meet relevant needs.

Furthermore, several points for improvement were identified in relation to the specific themes of the study.

There are two main legal instruments specifically designed to further information exchange: the Swedish Framework Decision and the Prüm Decision. Both have yet to be fully implemented by Member States. There has been progress in the implementation of the **Swedish Framework Decision** (SFD): most Member States have transposed it. However, it is still not being fully applied, hence it is failing to achieve its full potential. An important factor hampering the application of SFD is the fact that Single Point of Contact (SPOC) officers and field officers are only aware of it to a limited extent. Rather than it being understood that the SFD is a legal tool, the SFD is mostly associated with the forms to be used and these are generally considered too cumbersome. While the forms are hence very rarely

used, many consider the SFD not as a practical tool, but as a horizontal principle of information exchange. The time limits are considered useful and are complied with in most cases. However, the obligatory channelling of requests through SPOCs in some Member States is *de facto* detrimental to the principle of equivalent access, because the distance between the source and end-user of information is extended. On the other hand, refusals to provide information are rare.

Due to low prioritisation in several Member States, the implementation of the **Prüm Decisions** is still not as advanced as it should be. Procedures to follow up on Prüm hits are not clearly defined in the Member States. There is currently also an ambiguity among practitioners regarding whether SFD should be used for Prüm follow-up or not. Interpol seems to be the channel that is used most frequently for Prüm follow-up, but most officers use different channels depending on the specific case.

The vast majority of Member States have an international police cooperation structure that at least partly complies with the **Single Point of Contact** (SPOC) criteria set by the EIXM Communication and the subsequent SPOC Guidelines. However, application of the SPOC concept varies across Member States. Although the adoption of the Guidelines seems to have inspired reflection among Member States on how to adapt the organisation of their SPOC, this process remains voluntary and hence limited in scope.

The actual **choice of channel** through which an information exchange request is communicated currently depends on many factors, which are not consistent across and not even within Member States. Instructions on the choice of channel exist at EU level and in most Member States, but personal considerations, including preferences for a certain channel, also play a major role in the actual choice. The unstructured choice of channel causes complexity for the SPOC and generates risks for the quality of the data.

As concerns the actual use of the different channels, the Europol channel is by many wrongly seen to be confined to the Europol mandate. The Interpol channel is currently used in many cases when only EU Member States are concerned. The SIS II communication channel is in some Member States still used for exchanges under Article 39 of the Convention implementing the Schengen Agreement and under the SFD although legally no longer permissible.

Europol's SIENA tool is currently used in most Member States, but not to the same extent. Only a very few Member States have started to promote it as the main channel for EU information exchange. Several hurdles still exist, notably the lack of 24/7 availability in the Member States, the fact that SIENA is in most Member States not yet connected to the case management system, as well as low awareness of and sceptical attitudes to SIENA.

There is seemingly a business need within the law enforcement area for **extended sharing of information** within the EU. One obstacle to such an extension are the rules for entering data in the Europol Information System (EIS), the limited user community and the fact that EIS data is normally not easily accessible on a larger scale in operational police work. This also leads to a vicious circle where the volumes of data in EIS are too small for Member States to invest in resources and solutions to increase their use of it.

For existing and future extensions of information exchange, the Universal Messaging Format (**UMF**, implemented in SIENA and which can be used for Prüm and SFD) is seen as essential, in particular for instruments where other standards do not yet exist. The implementation of UMF II is making rather slow progress, mainly due to budgetary issues but also due to the short time that has elapsed since the standard was launched. There is however a quite high interest among Member States to proceed with implementing it and also to follow the creation of UMF III, i.e. the next version of UMF, extending its functions.

There are currently a range of different actors at national and EU level providing numerous **training** courses on information exchange. Nevertheless, while individual activities have generally been appreciated by participants, there is currently no overarching strategy at EU and national level. At EU level, a Communication on a European Law Enforcement Training Scheme (including aspects on information exchange) has been adopted. However, most of its action points have not yet been pursued further, mainly due to a lack of resources and the relocation of CEPOL. Moreover, many Member States do not have a training strategy identifying needs and rather offer training on an ad hoc basis. Specific shortcomings have been identified in relation to initial training at police academies, on-boarding for SPOC officers and on-going training for SPOC and field officers.

Specific recommendations regarding the individual themes of the study are provided in the report under each subsection of Chapter 4.

1 Introduction

The Commission's Directorate-General Home Affairs (DG HOME) mandated Deloitte, as a request for services under tender No HOME/2012/ISEC/PR/025-A3, to conduct a study on the implementation of the European Information Exchange Model (EIXM) for strengthening law enforcement cooperation.

The purpose of the study was to provide a follow up to the EIXM Communication[1] and to survey and assess activities carried out in Member States in this context as well as point to possible ways of further improvement.

This report constitutes the **Final Report** of the study on EIXM and presents:

- A description of the methodological approach (section 2);
- The legal and policy context, the instruments and their key operational features (section 3);
- An analysis of implementation of EIXM (section 4); as well as
- The following Annexes:
  - Annex 1: Analytical Framework;
  - Annex 2: Interview Guides; and
  - Annex 3: Glossary of terms.

[1] Communication from the Commission to the European Parliament and the Council, *Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)*; COM(2012) 735; http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/docs/20121207_com_2012_735_en.pdf.

2 Scope and methodology of the study

2.1 Scope of the study

Our assessment of the implementation of the European Information Exchange Model (EIXM) landscape focused on the following aspects of EIXM[2]:

Chapter 3:

Context

The legal and policy frameworks:

- The Treaty objectives;
- The policy instruments; and
- The relevant articles of the European Charter on Fundamental Rights.

The information exchange instruments:

- The Swedish Framework Decision; and
- The Prüm Decisions.

The processes and practical aspects of information exchange

Chapter 4:

The implementation of the European Information Exchange Model (EIXM)

Implementation of the legal instruments:

- The Swedish Framework Decision; and
- The Prüm Decisions.

Processes and practical aspects of information exchange:

- The Single Points of Contact (SPOCs);
- The channels used for information exchange;
- The use of instruments to exchange data from national police records; and
- Technical developments beyond UMF II.

Horizontal challenges of EIXM

- Training measures; and
- Further general considerations.

[2] These were also covered in the Commission's 2012 EIXM Communication.

2.2 Our methodology

We carried out the study in three phases:

1. The **Structuring phase** allowed our team to structure the study according to specific research questions to be answered according to the general and specific objectives stipulated in the Terms of Reference (ToR). This phase ended with the submission and validation of the Inception Report. This phase mainly served to develop the methodological tool that we use to structure all our assignments, namely the Analytical Framework. The Analytical Framework was hence used as the backbone of our project delivery.

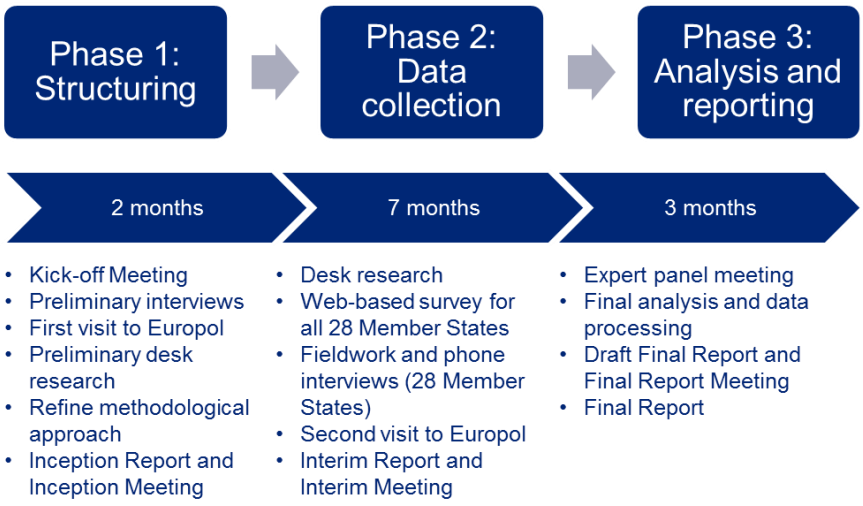
2. The study's **Data gathering phase** aimed to collect data to respond to the research questions developed in the Inception Report and was carried out through the research activities detailed in our project plan, including data collection at European and national levels (based on desk research, an EU-wide web-based survey, as well as fieldwork in a selection of 12 Member States and telephone interviews in the remaining 16 Member States).

3. The **Analysis, judgement and reporting phase** is horizontal in that relevant activities occur at different times during the project implementation. The study team analysed data both during and after completion of each research activity.

   A final analysis and judgement took place at the last phase of this assignment to produce the Final Report including our conclusions and recommendations for future actions. This consisted of going back to the Analytical Framework to ensure that we have met each objective of the study and given an answer to every research question. This exercise was crucial to the analysis and ensured that conclusions and recommendations, based on a triangulation of the data gathered, were strictly evidence-based.

We present in the Figure 1 a synthesis of the work plan of our study.

Figure 1: Work plan of the study



3 Context

We present in this section the frameworks which provide the legal basis for information exchange, including the two specific legal instruments, the Swedish Framework Decision and the Prüm Decisions. This chapter is based on the results of our desk research and inputs received during strategic interviews carried out during the first phase of the project. The following chapter will deal with how the specific instruments have been transposed and are being implemented in practice, together with consideration of information exchange in day-to-day practice.

3.1 EIXM – the rationale

Smooth and secure cross-border information exchanges between law enforcement authorities are essential in order to ensure a high level of security in the EU and tackle serious and organised crime, as well as other offences that require cross-border collaboration. Furthermore, in order to combat crime efficiently, investigating services need to know without delay whether and what information is available in other Member States. In order to ensure timely access to accurate and up-to-date data for law enforcement authorities, a considerable number of EU instruments and systems have been put in place in recent years. International and bilateral arrangements have supplemented this EU action.

In the light of the rather complex and diverse landscape of instruments described later in this chapter, the Commission was invited by the Stockholm Programme[3] to assess the need for a European Information Exchange Model (EIXM) following the general principles of the Council's Information Management Strategy of 2009[4].

The work on EIXM involved, as a starting point, a mapping exercise and evaluation[5], focusing on the following aspects of cross-border information exchange in the EU and the four EFTA countries[6]:

- The legal dimension, including EU and national legislation regulating cross-border exchange of information and criminal intelligence;
- The communication channels through which information and criminal intelligence are exchanged;
- The actual flow of information and criminal intelligence between relevant key players; and
- The technical solutions (databases and IT solutions) used to exchange information and criminal intelligence.

Based on the results of this work, which was presented in different reports, the 2012 'EIXM Communication' on *Strengthening law enforcement cooperation in the EU: the European Information*

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010XG0504(01)&from=EN.
[4] Council Conclusions on an Information Management Strategy for EU internal security 2979th Justice and Home Affairs Council meeting Brussels, 30 November 2009; http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/111549.pdf.
5 Strengths and weaknesses as regards cross-border sharing of law enforcement information were also emphasised in the European Information Exchange Model – Conclusions of the Information Mapping Exercise of 2010, which focused on the Swedish Framework Decision and the Prüm Decision.
[6] C.f. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/eixm/index_en.htm.

Exchange Model (EIXM)[7] took stock of the state of play. It then provided recommendations for improvements. Its main conclusion was that existing instruments and channels for the exchange of law enforcement information should be improved rather than developing and putting in place new instruments and databases. The present study builds on this information and provides a further assessment of national activities. Based on this assessment, concrete recommendations to address weaknesses and improve the level of compliance with the EIXM recommendations[8] or possible alternatives are provided.

In order to achieve the objectives of this study, it is imperative to have a good understanding of the current landscape of information exchange activities between law enforcement authorities and the key aspects that make up this "landscape", taking account of the findings of the previous studies.

In line with the EIXM Communication, such aspects include the **legal instruments**, the **communication channels and tools** used for cross-border exchange of information, the **key players** involved and the **information flows**.

The **instruments** for information exchange are various types of concrete EU measure or system put in place to ensure smooth communication between law enforcement authorities across borders. The key instruments are:

- The Swedish Framework Decision (SFD)[9], which covers the exchange of information for the purpose of criminal investigations or criminal intelligence operations, with a particular focus on access to information;
- The Prüm Decision[10] , which provides for automated exchange of biometric data (DNA profiles and fingerprint data) and vehicle registration data for the prevention and investigation of criminal offences and maintaining public security[11];
- The Schengen Information System (SIS (II))[12] which provides alerts on persons and objects; and
- The Council Decision establishing the European Police Office (Europol)[13], which provides for the collection, storage, processing, analysis, and exchange of information and intelligence as one of Europol's principal tasks.

We introduce the policy framework and relevant practical aspects in this chapter, but before doing so, we describe the overarching frameworks in the Treaty and policy. The next Chapter discusses implementation of the instruments and the broader practice of information exchange.

---

[7] COM (2012) 735 final (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0735:FIN:EN:PDF).
[8] The recommendations are reiterated per topic at the start of every section in chapter 4.
[9] Council Framework Decision 2006/960 JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.
[10] Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.
[11] The following information is exchanged: Prevention of data – fingerprint (FP) and vehicle registration data (VRD); investigation of criminal offences – DNA, FP, VRD; and maintaining public security – VRD.
[12] Cf. Council Decision No 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).
[13] Council Decision 2009/371/JHA establishing the European Police Office (Europol) (see: https://www.europol.europa.eu/sites/default/files/council_decision.pdf).

3.2 EIXM – the legal and policy underpinning

The instruments described above fall within overarching objectives set by the Treaty and specific policy frameworks described below and have to be applied with respect for fundamental rights. This section discusses:

- The relevant Treaty objectives that provide the legal basis for action in this field;
- The policy frameworks deriving from the Treat objectives; and
- Relevant Articles of the European Charter of Fundamental Rights.

3.2.1 The Treaty provisions

The effective elimination of internal borders in the EU and subsequently the ease of crime to spread have increased the need for a coordinated system of cooperation with regard to judicial, police, and related administrative matters. This is recognised by Article 87 of the Treaty on the Functioning of the European Union (TFEU), which established the legal basis for EU action in relation to information exchanges between law enforcement authorities: "The Union shall establish police cooperation involving all the Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences." This includes the possibility of establishing measures in the following three areas, of which the first [87(2)(a)] is the most important for the purpose of this Study:

- Collection, storage, processing, analysis and exchange of relevant information;
- Support for the training of staff, and cooperation on the exchange of staff, on equipment and on research into crime-detection; and
- Common investigative techniques in relation to the detection of serious forms of organised crime.

In view of the sometimes overlapping role of the police and the judiciary (since in some countries judicial authorities carry out tasks that are done by police in other countries as discussed below), other Treaty provisions e.g. on judicial cooperation also play a role in this field, as well objectives relating to the exchange of information in specific areas, such as asylum and migration or customs.

It is important to note that the Treaty framework relating to law enforcement cooperation has undergone substantial changes. By moving the former 'Third Pillar' (police and judicial cooperation) from the Treaty on European Union to the TFEU, the Treaty of Lisbon altered the modalities of law making and enhanced judicial review by the Court of Justice of the EU (CJEU) in the area of Justice and Home Affairs. It is expected that this will have positive effects on the standard of judicial review in this area. In this regard it needs to be noted, however, that the CJEU may not review the validity or proportionality of operations of national law enforcement authorities (Article 276 TFEU), as this is related to the core of the functions of the state of safeguarding security (cf. Articles 4 and 72). Consequently, national courts and the European Court of Human Rights will play an important role with regard to judicial review in the law enforcement sector as well. In addition, the Commission was granted new powers with respect to the enforcement of the rules covered by this policy area. In particular, as of December 2014 it is possible for the Commission to start infringement proceedings in case of non-compliance.

The Lisbon Treaty also made the Charter of Fundamental Rights of the European Union (the Charter)[14] legally binding (Article 6 TEU), thus strengthening fundamental rights, including data protection. The

[14] OJ C 326, 26.10.2012, p. 391. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:0391:0407:EN:PDF).

fundamental rights and data protection provisions that are relevant with regard to information exchange in the law enforcement sector are further discussed in section 3.2.3.

3.2.2 Policy frameworks for the exchange of law enforcement information

This sub-section describes the policy framework that has been established based on the Treaty provisions, including actions and objectives set out in the so-called Hague[15] and Stockholm Programmes, the Council's 2009 Information Management Strategy and the related Action Plans, as well as Commission Communications and studies.

3.2.2.1 The Hague and Stockholm Programmes

In 2005, the Hague Programme introduced the principle of availability, according to which information for law enforcement purposes needed by authorities of one Member State are made available by the authorities of the Member State where the information is stored. The European Council stressed that the following conditions should be observed in the implementation of the principle of availability:

- The exchange may only take place in order for legal tasks to be performed;
- The integrity of the data to be exchanged must be guaranteed;
- The need to protect sources of information and secure the confidentiality of the data at all stages of the exchange, and subsequently;
- Common standards for access to the data and common technical standards must be applied;
- Supervision of respect for data protection, and appropriate control prior to and after the exchange must be ensured; and
- Individuals must be protected from abuse of data and have the right to seek correction of incorrect data.

While building on the objectives of its predecessors, the Stockholm Programme[16] in 2010 shifted the focus from the prime objective of combating terrorism and organised crime to widespread cross-border crime that has a significant impact on the daily life of the citizens of the EU, e.g. also cybercrime. The Programme identified Europol as the main "hub" for information exchanges between the Member States' law enforcement authorities. In this way, the Stockholm Programme not only called for a "business driven development, a strong data protection regime, interoperability of IT systems and a rationalisation of tools as well as overall coordination, convergence and coherence"[17], but also for the examination of how to ensure that Europol receives information from Member States' law enforcement authorities and how operational police cooperation can be stepped up, e.g. as regards incompatibility of communication systems and other equipment. Finally, the Stockholm Programme emphasised the need for the adoption of a decision on the modalities of cooperation, including on the exchange of information between EU agencies. Hence, the use and interoperability of various channels for the exchange of law enforcement information between Member States' authorities and EU bodies in order to make crime prevention and the protection against serious and organised crime more effective is at the heart of the Stockholm Programme.

Like its predecessors, the Stockholm Programme was supported by the development of an Action Plan[18] for the implementation of the objectives within a given timeframe. The Plan lays down the basis for the implementation of an Internal Security Strategy[19], implying a coordinated approach to police

[15] C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:053:0001:0014:EN:PDF.
[16] C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF.
[17] C.f. http://register.consilium.europa.eu/pdf/en/09/st16/st16637.en09.pdf.
[18] C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF.
[19] The related EU Communication COM(2010) 673 sets out five strategic objectives: (1) Disrupt international criminal networks, (2) Prevent terrorism and address radicalisation and recruitment, (3) Raise levels of security for citizens and

cooperation border management, criminal justice cooperation and civil protection. In order to improve the exchange of information between relevant public bodies, the Action Plan requires an overview of existing data collection, processing and data-sharing systems, with a thorough assessment of their usefulness, efficiency, effectiveness, proportionality and their respect of the right to privacy in order to develop a consolidated and coherent mechanism for future information exchange. In relation to the need for improved exchange of information, the Action Plan, for example, laid the groundwork for the European Commission Communication on the overview on information collection and exchange[20] and the Communication on the European Information Exchange Model[21]. Further action in this area is based on the Council's Information Management Strategy followed by another Action Plan discussed in the next section.

3.2.2.2 The Council's Information Management Strategy

In order to remedy the current situation of an "uncoordinated and incoherent palette of information systems and instruments", which has "incurred costs and delays detrimental to operational work"[22], the incoming Swedish Presidency submitted a proposal to the Ad Hoc Working Group on Information Exchange for an Information Management Strategy in June 2009.[23] The aim of the strategy was to define how information should be stored and exchanged, as well as how the process should be managed. Thus, the document provides guidance on how to ensure an appropriate information exchange where supply of information takes account both of business needs and the rights of the individual in order to assist law enforcement authorities in how to efficiently organise an effective cross-border exchange of information.

The strategy was updated in Council conclusions under the Italian Presidency at the end of 2014[24].

The strategy consists of the following focus areas:

- Needs and requirements:
  - Needs, requirements and added value are assessed as a precondition for development;
  - Development follows agreed law enforcement workflows and criminal intelligence models;
  - Development supports both data protection requirements and business operational needs;
- Interoperability and cost efficiency:
  - Interoperability and co-ordination are ensured both within business processes and technical solutions;
  - Re-utilisation is the rule: do not re-invent the wheel;
- Decision-making and development processes:
  - Member States are involved from the very start of the process;

businesses in cyberspace, (4) Strengthen security through border management, and (5) Increase Europe's resilience to crises and disasters.

[20] C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF.

[21] C.f. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/docs/20121207_com_2012_735_en.pdf.

[22] See the report of the Future Group of Ministers of Home Affairs.

[23] C.f. http://register.consilium.europa.eu/pdf/en/09/st16/st16637.en09.pdf.

[24] C.f. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015701%202014%20REV%201.

- There is a clear responsibility for each part of the process, ensuring competence, quality and efficiency; and

- Multidisciplinary approach: multidisciplinary coordination is ensured within the Justice and Home Affairs (JHA) area.

3.2.2.3 European Commission Communication on the Overview of Information Management

In 2010, the European Commission published a Communication concerning an overview of information management in the area of freedom, security and justice.[25] The Communication provides a synthesis of EU-level measures regulating the management of personal information and proposes a set of principles for the development and assessment of such measures in order to make the approach to the exchange of information more coherent.

The Communication covered information exchange instruments that facilitate the exchange of personal data and were at that time (1) either currently in force, under implementation or consideration, or (2) set out in the Stockholm Programme Action Plan. The table below includes the instruments that were covered in the Communication. It was adapted so as to represent the changes since 2010. Instruments that are highlighted as part of the specific objectives in the Terms of Reference for this study are marked in bold.

Table 1: Instruments of information management currently in place[26]

Objective	Instruments
Instruments either currently in force, under implementation or consideration	
Aiming to enhance the operation of the Schengen area and the customs union:	• Second Generation Schengen Information System (SIS II); • EURODAC; • Visa Information System (VIS); • Advanced Passenger Information System (API); • Naples II Convention; • Customs Information System; and • Customs file identification database (FIDE).
Aiming to prevent and combat terrorism and other forms of serious cross-border crime	• **Swedish Framework Decision;** • **Prüm Decision;** • European Criminal Records Information System (ECRIS); • Financial Intelligence Units (FIUs); • Asset Recovery Offices (AROs); • Cybercrime Alert Platforms; • European Police Office (Europol); and • European Union's Judicial Cooperation Unit (Eurojust).
Aiming to prevent and combat terrorism and other forms of serious transnational crime	• Passenger Name Record (PNR); and • Terrorist Finance Tracking Program (TFTP).

[25] COM(2010)385, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF
[26] This table is based on the Overview Communication but has been adapted by the authors of this study.

Objective	Instruments
Instruments set out in the Stockholm Programme Action Plan	
Legislative proposals to be presented by the Commission	• Passenger Name Record package; • Entry/Exit System (EES); and • Registered Travellers Programme (RTP).
Initiatives to be studied by the Commission	• EU terrorist finance tracking system; • Electronic System of Travel Authorisation (ESTA); and • **European Police Records Index System (EPRIS).**

A central finding of analysis of the above instruments in the Communication is that the exchange of law enforcement information in the EU is characterised by:[27]

- A decentralised structure;
- Limited or unitary purposes of various instruments;
- Potential overlaps of their function;
- Differentiated control and access rights according to the logic of different law enforcement communities;
- Variable data retention and security rules, as well as identity management principles; and
- Divergent review mechanisms. Hence, the conclusion of a divergent landscape with regard to information collection and exchange instruments is at the heart of the Communication.

3.2.2.4 Schengen evaluation and governance

Council Regulation 1053/2013[28] covers the establishment of an evaluation and monitoring mechanism to verify the application of the Schengen *acquis*. This Schengen Evaluation Mechanism (SEM) will provide an opportunity to verify the application of the Schengen *acquis* in the field of law enforcement cooperation, including the way information is exchanged and how communication takes place.

Apart from the core of the Schengen *acquis* (Schengen Convention, Schengen Information System) the SEM will also look into the practical use of the SFD, Prüm, Europol tools and the concepts of EIXM (e.g. SPOCs). As an example of this function of the SEM, the standard questionnaire for Member States, drawn up in July 2014, contains questions related to police cooperation and information exchange. The SEM could therefore also partly be an instrument for verifying the implementation of the EIXM recommendations.

[27] The detailed findings of this Communication will further inform the analysis of the information exchange mechanisms and channels relevant in the context of the EIXM.

[28] Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R1053&from=EN.

3.2.3 Relevant provisions in the Charter of Fundamental Rights and data protection legislation

As indicated above, the Lisbon Treaty rendered the **European Charter of Fundamental Rights** binding by means of Article 16 of the TFEU.[29] According to Article 51, the Charter is applicable to institutions, agencies and other bodies of the Union, as well as to Member States when they are implementing EU law. The Charter includes a number of Articles that are relevant to law enforcement cooperation and the fight against cross-border crime. The most pertinent Articles are:

- Right to liberty and security (Article 6);
- Respect for family and private life (Article 7); and
- Protection of personal data (Article 8).

While Article 6 ensures the security of persons within the European Union and thus can be seen as a plea for (cooperative) law enforcement mechanisms in itself, Articles 7 and 8 set the boundaries for public authorities' competences by stipulating everyone's right to respect for his or her private and family life, home and communications, and the right to the protection of personal data. Hence the European Charter of Fundamental Rights can be seen both as an enabler and limiter of cross-border law enforcement cooperation and the related information exchange mechanisms.

Article 8 of the EU Charter states that personal data must be processed fairly for specified purposes, and that must either be on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules is subject to control by an independent authority.

In addition, the Charter includes a number of citizens' rights (Title V) and judicial rights (Title VI). Article 41 is particularly relevant as it which lays down the right to good administration. On the basis of Article 41, everyone has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the Union handle his or her affairs impartially, fairly and within a reasonable time. This includes e.g. the right to be heard. Judicial rights include for example the right to an effective remedy, as stipulated in Article 47.

Article 52 lays down rules on the scope and interpretation of the provisions contained in the Charter. Accordingly, the rights should be interpreted in the light of the corresponding Treaty provisions (where applicable), taking into account the explanations attached to the Charter as well as relevant case-law of the European Court of Human Rights. Article 52(1) provides for general rules to restrict the rights guaranteed by the Charter. Limitations can be made to protect a "general interest recognised by the Union or […] the rights and freedoms of others." Any limitation must be necessary and proportionate, and prescribed by law, maintaining the essence of the right concerned.

While the data protection provisions in the EU Charter and the TFEU apply to all EU policy areas, it is recognised under EU law that the specific nature of the field of law enforcement cooperation may call for tailored data protection rules.[30]

As regards the general data protection framework, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[31] is the central instrument in the EU. It specifies general data protection principles that had previously been agreed

[29] OJ C 326, 26.10.2012, p. 391. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:0391:0407:EN:PDF)
[30] Declaration (No. 21) on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, OJ. C 83, 30.3.2010, p. 344.
[31] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

upon in a Council of Europe Convention.[32] The Directive also required Member States to set up specialised and independent authorities to ensure that the data protection rules are observed (Article 28). Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies[33] complements the Directive and established the European Data Protection Supervisor (EDPS) to fulfil the role of an EU independent supervisory authority. A proposal to amend the Directive was put forward by the European Commission in 2012[34].

To ensure that the specific needs of the law enforcement sector were taken account of, 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 matters[35] was adopted. It contains rules on data processing, data transmission, rights of the data subject and safeguards ensuring data quality, security, and protection. The implementation of this document is still ongoing. By 9 November 2011, 14 Member States had indicated that they had legislation in force to implement the Framework Decision, and two had indicated that they had no need to transpose the Decision.[36]

The Framework Decision has been subject to criticism as regard its effectiveness. The Commission has in particular pointed out that its limited scope is the source of problems, in particular because the Decision only applies to cross-border data processing activities[37]. Domestic data processing activities are thus assessed on the basis of national data protection provisions, although it is often difficult to distinguish between the two categories. Moreover, the Decision does not apply to instruments enacted at EU level that already have a tailor-made data protection approach in place. This creates a wide landscape of different rules. As part of the review of the data protection framework, the Commission proposed a Directive on 28 January 2012 to enhance the data protection rules in this area.[38]

In addition to the general data protection framework applicable in the framework of police and judicial cooperation, there are rules that are applicable to specific instruments, which are enshrined in the relevant legal bases.[39] In the EIXM Communication, the Commission underlined that in cases that involve sequential use of more than one instrument, care needs to be taken to ensure that the rules on data protection of each instrument are to be respected.[40]

In its opinion on the EIXM Communication, the EDPS underlined the importance of taking data protection into account when further developing EIXM. As technology changes, the interoperability between different databases may pose challenges to data protection. In this regard, the EDPS pointed to the importance of the data protection principle of purpose limitation, which states that data may only be used for the purpose of its original collection.[41]

---

[32] Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm).
[33] C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:EN:HTML.
[34] C.f. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
[35] C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0977:EN:NOT.
[36] COM(2012) 12 final (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0012:FIN:EN:PDF).
[37] COM(2010) 609 final (http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf), pp. 13, 14.
[38] COM (2012) 10 final.
[39] See e.g. Chapter 6 of the Prüm Decision as well as the Europol Council Decision.
[40] EIXM Communication, p. 6.
[41] Opinion of the European Data Protection Supervisor on the EIXM Communication (https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-04-29_EIXM_EN.pdf).

3.3 EIXM – the legal instruments

This section is an introduction to the formal aspects and main features of the legal instruments which are the focus of this study:

- The Swedish Framework Decision; and
- The Prüm Decisions.

3.3.1 The Swedish Framework Decision

In the light of the terrorist attacks in Madrid and London, in 2004 and 2005, Sweden proposed an initiative to simplify the exchange of information and intelligence between law enforcement authorities.[42] The so-called **Swedish Framework Decision** (SFD)[43], adopted in 2006, sets out common rules on procedures according to which information may be exchanged between Member States' law enforcement authorities.

The essence of the Decision is that Member States must ensure that the conditions applied to providing and requesting information and intelligence to or from competent law enforcement authorities from other countries are not stricter than those applicable at national level (Article 3). This is referred to as the **principle of equivalent access**, which is considered as a major step forward in cross-border law information exchange[44]. By establishing relevant conditions for the provision of information and intelligence, the Swedish Framework Decision partly implements the principle of availability established in The Hague Programme[45]. Notably, Article 4 stipulates **time limits** for providing information.[46] If the time limits cannot be kept to, the Member State receiving the request is required to provide reasons for not being able to comply. In addition, the Decision seeks to **promote information exchange with Europol and Eurojust** for crimes that fall within their mandates.[47]

While Member States are obliged to share relevant information with other Member States, there are certain limits are enshrined[48] in the Decision. In particular, the Decision does not include an obligation for Member States' law enforcement authorities to collect information in order to be able to answer queries from other national or EU bodies. Moreover, information may be used as evidence as part of a judicial procedure[49] only if the source Member State has given its consent (Article 1). In addition, the SFD provides grounds to refuse information, for example on the grounds of national security interests (Article 10).

---

[42] C.f. http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf.
[43] Framework Decision 2006/960 JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:EN:PDF.
[44] C.f. http://www.eumonitor.nl/9353000/1/j4nvgs5kjg27kof_j9vvik7m1c3gyxp/vj6iponbr3yj/f=/14755_1_12_rev_1.pdf.
[45] C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:053:0001:0014:EN:PDF.
[46] Accordingly, urgent requests shall be responded to in eight hours, Non-urgent cases shall be responded to within one week. In all other cases, information shall be provided within 14 days.
[47] Cf. Article 6(2) SFD.
[48] In practice, these forms are rarely used and their added-value has been questioned by a number of stakeholders. This is discussed in section 4.1.1.2 *Operational compliance with the Swedish Framework Decision's legal requirements*.
[49] It is noted that the recent adoption of the European Investigation Order (Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters) will influence the judicial aspects of law enforcement information exchange, as further explained in this section.

Finally, the SFD incorporates **forms** which may be used by law enforcement authorities for the exchange of information. Annex A of the SFD contains a form to be used for transmitting requested information and Annex B contains a form to request information.

3.3.2 The Prüm Decisions

The cooperation that started as a multilateral treaty between Austria, Belgium, France, Germany, Luxembourg, the Netherlands and in 2005, i.e. the Prüm Convention[50], was shifted to EU level with Council's Decision 2008/615/JHA[51] and the related provisions for its implementation 2008/616/JHA[52] (the two 'Prüm Decisions'). The Prüm Decisions set out provisions regarding:

- Automated search of data;
- Supply of data in relation to major events;
- Supply of information in order to prevent terrorist offences; and
- Other measures for stepping up cross-border police cooperation.

They include the obligation to establish databases related to automated DNA analysis files, automated dactyloscopic (i.e. fingerprint) identification systems[53], and vehicle registration data[54], as well as procedures and modalities for Member States' access to each other's databases in the context of cross-border law enforcement.

3.4 EIXM – the processes and practical aspects of information exchange

In this section we discuss the key operational features and players in implementation of EIXM.

The 2012 EIXM Communication discussed the three main EU and international **communication channels** used for cross-border information exchange. The communication channels used involve different types of national unit and/or authority in each Member State. The national units may be, but are not restricted to, Single Points of Contacts (SPOC).[55] In addition, there are other channels within the EU, such as bilateral Liaison Officers (who are distinct from Europol liaison officers), specific sectorial channels, and Police and Customs Cooperation Centres (PCCCs) in border regions.

The channels are designed for different purposes and use different communication tools:

- The **Europol channel** offers exchange via the National Units and the Europol liaison officers. SIENA[56] is the corresponding communication tool. Exchanges via the Europol channel do not

[50] Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, c.f. http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.
[51] C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:0011:EN:PDF.
[52] C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF.
[53] This has enabled law enforcement authorities within the Member States, for example, to compare DNA profiles and fingerprints found at crime scenes with (anonymised) database entries in databases of all Member States. In a second step, specific related personal data can be requested from the Member State administering the file in order to match the crime evidence with the database information. The procedure is run through a designated national contact point in each Member State, i.e. an intermediate institutions that national officials have to contact in order to proceed with data comparisons.
[54] Car registration data (including licence plates and chassis numbers) are exchanged through national platforms that are linked to the online application EUCARIS.
[55] The term SPOC is used in this study to refer to international police cooperation units in the Member States, without implying that these fulfil all the criteria set at EU level. Further information about the concept can be found in section 4.2.1 *The Single Points of Contact (SPOCs*).
[56] Secure Information Exchange Network Application.

need to be related to Europol's mandate, but could also be related to other crimes of bi- or multilateral concern.

- The **Interpol channel** is generally mainly meant for exchanges involving third countries. Information is exchanged via the Interpol National Bureaux, using the communication tool I-24/7.
- The **SIRENE Bureaux**[57] are responsible for exchanging information related to or supplementary to SIS data. SIRENE Bureaux use the SIS II communication network as communication tool.
- The **PCCCs** are the central contact points for border regions. They mainly deal with regional cases with a cross-border element. Cases the PCCC deals with revolve, for example, around serious and sometimes organised crime, burglary or stolen vehicles.

The following table provides a brief comparison of the three main channels and additional bilateral channels in terms of the tools used, the legal basis and whether the choice of channel is compulsory under EU law or not.

Table 2: Main channels for the cross-border exchange of law enforcement information

Office/Unit responsible	Tool/network used	Legal basis	Choice of channel
Europol National Units	SIENA (developed within Europol but not specifically mentioned in the legal basis)	Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office	Compulsory
Interpol National Central Bureaux	I-24/7	n/a	Not compulsory in most situations[58]
SIRENE Bureaux	SIS II network	1. Council Regulation 1987/2006 of the EP and COUNCIL of 20/12/2006 on the establishment, operation and use of the second generation SIS (SIS II); 2. Council Decision 2007/533/JHA of 12 June 2007 on establishment, operation and use of the second generation SIS (SIS II); and 3. Commission Decision adopting SIRENE Manual, 26 February 2013.[59]	Compulsory
Bilateral Liaison Officers	Diverse	Bilateral agreements	Depends
National contact points, e.g. Police and	Diverse	Based on the legal provisions for the other channels and tools in order to implement national contact points	Depends

[57] Supplementary Information Request at the National Entry. SIRENE Bureaux are national coordination offices in the participating countries that provide supplementary information on alerts and coordinate measures in relation to alerts in the Schengen Information System (SIS). (http://www.consilium.europa.eu/policies/justice-et-affaires-interieures-%28jai%29/schengen).

[58] There is an obligation for EU Member States to exchange passport data with Interpol in certain situations, as set out in Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005E0069).

[59] C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:071:0001:0036:EN:PDF.

Office/Unit responsible	Tool/network used	Legal basis	Choice of channel
Customs Cooperation Centres[60]			

Clearly, there is great diversity in terms of the measures (instruments, channels and tools) that have been put in place, with each of them designed for a specific purpose. An investigation may thus involve parallel or sequential use of more than one instrument or channel. The choice of information channel is only partly regulated by EU legislation. Specific rules apply to operating the channels and tools related to Interpol.

Two of the main legal bases for information exchange, the SFD and the Prüm Decisions (discussed in the previous section), do not include a definition of the choice of channel. On the other hand, supplementary information following hits with alerts in the SIS must be followed up by the SIRENE office via the dedicated SIS II channel.

As far as the **key players** are concerned, the EIXM Communication refers to *law enforcement* cooperation without strictly defining the scope. No common EU definition of "law enforcement authorities" exists, and the players involved in investigations in different Member States may vary. According to the *Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments*[61] law enforcement authorities "typically include police units and competent authorities such as Gendarmerie, Customs and Excise authorities, Border Guards and Coast Guards, but individual agency responsibilities and organisational procedures often vary between MS." The **involvement of the judicial authorities**, including prosecutors, at various stages of the criminal justice process varies between the Member States. This has implications for the need to apply Mutual Legal Assistance (MLA) procedures, which impacts on information exchange.

From a **technical perspective**, the effective and efficient exchange of law enforcement information depends on the availability and interoperability of up-to-date IT infrastructure. Issues such as, for example, fast, stable, and secure network connections as well as IT access management and software upgrades are as important as the interoperability of technical and administrative standards within the Member States, e.g. with regard to the implementation of the Universal Messaging Format II (UMF II) standard.

There is seemingly a business need for extended sharing of information within the EU, namely to exchange information from national police records. To this end, the Commission examined whether the introduction of a **European Police Records Index System** would be desirable. In the EIXM Communication, it is highlighted that the identified business needs could partly or fully be solved by existing instruments that are currently not used to their full potential. Thus, the introduction of a new system was not considered necessary.

Specialised information exchange **training** for law enforcement staff is currently provided through Europol and the European Police College (CEPOL). SIRENE training programmes are also carried out on a regular basis in cooperation between the Commission, CEPOL, the European Agency for the

[60] Established on the basis of the 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 checks at their common borders.

[61] C.f. http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/icmpd_study_lea_infoex.pdf (p. 16).

operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) and Member States. The training relates to the practical and technical aspects of information exchange. In addition, exchanges of staff are offered at the EU level.

The EIXM Communication highlights that respect for **fundamental rights**, including the right to **data protection and privacy**, is a horizontal issue to be taken into consideration in the context of law enforcement information exchange. This includes, for example, to the collection, storage and sharing of personal data. It is therefore relevant to consider the provisions in primary legislation and general data protection instruments, as well as specific rules on data protection that apply to the individual instruments of information exchange.[62]

The EIXM Communication concludes – based on the numerous studies on the functioning of the existing activities – that cross-border information exchanges generally work well. However, while the EIXM Communication concludes that no new EU level law enforcement database or instruments are currently needed, it pointed to some necessary improvements, making the following recommendations: (1) improve the use of existing instruments, (2) streamline and improve the management of the channels, (3) ensure better data quality, security, and protection, (4) improve training and awareness for and among law enforcement officials, and (5) increase the use of available funding opportunities.[63] More specifically, the gaps it identified related in particular to:

- The Member States have not fully implemented the Swedish Framework Decision (e.g. with regard to the principle of equivalent access[64]) and the Prüm Decision;
- The law enforcement authorities have different approaches to the choice of channel and therefore different channels are used to different extents;
- Not all law enforcement authorities have developed national instructions for the choice of channel;
- Single Points of Contact (SPOCs) in the form of central coordination units have not yet been set up by all Member States;
- Technical interoperability under UMF II is not yet fully assured;
- Appropriate and in-depth training and participation in mutual exchange programmes is not always assured for law enforcement officials, in particular specialist officers;
- Increased use of funding opportunities under the 2014-2020 EU Internal Security Fund is imperative; and
- Prüm statistics need to be improved.[65]

Through its detailed recommendations, the Commission's Communication provides a "Model for guiding EU and Member State activity"[66]. The Commission is to provide adequate support, including funding and guidance for training measures.

---

[62] See section 3.2.3 *Relevant provisions in the Charter of Fundamental Rights and data protection legislation*.
[63] In order to ensure effective information exchange, Member States can make use of EU funding under the Prevention of and Fight against Crime Fund that was replaced by an EU Internal Security Fund as of 2014. Funding is available in particular in relation to the development and implementation of the UMF II standard and the implementation of Prüm.
[64] See section 2.3.1.
[65] As part of the technical operating system within which Member States law enforcement authorities and EU bodies can exchange relevant information, a specific secretariat, i.e. an organisation or Member State explicitly appointed for this task, can gather logged information on messages sent/received by all the participating Member States in order to produce statistical reports.
[66] See the EIXM Communication (http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/docs/20121207_com_2012_735_en.pdf), p. 2.

The EIXM underlines that the principles that were set out in the 2010 "Overview Communication"[67] applied to developing new initiatives and evaluating current instruments:

- *Substantive principles*: safeguarding fundamental rights, including data protection and privacy; necessity; subsidiarity; and accurate risk management.
- *Process-oriented principles*: cost-effectiveness; bottom-up policy design; clear allocation of responsibilities; and review and sunset clauses.

These principles have also been taken into account as part of the present study.

[67] Overview of information management in the area of freedom, security and justice; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF.

4 The implementation of the European Information Exchange Model (EIXM)

In this Chapter we first look at the **implementation of the legal instruments**:

- Implementation and operational compliance with the Swedish Framework Decision; and
- Implementation and operational compliance with the Prüm Decisions.

We then look at **information exchange in practice**, including the relationship with other instruments where applicable. We cover the following areas:

- The Single Points of Contact (SPOCs);
- The channels used for information exchange;
- The use of instruments to exchange data from national police records; and
- Technical developments beyond UMF II.

Finally, we present **horizontal challenges of EIXM**, including:

- Training measures; and
- Further general considerations.

The information in this chapter is the result of the data collection activities described in section 2.2, including in particular an EU-wide web-based survey, as well as fieldwork in a selection of 12 Member States and telephone interviews in the remaining 16 Member States.

Each section closes by summarising the main findings and presenting our recommendations for each topic.

4.1 Implementation of the legal instruments

4.1.1 Implementation and operational compliance with the Swedish Framework Decision

As outlined in section 3.3.1, the Swedish Framework Decision is the central legal basis for information exchange in the EU. In the EIXM Communication, the Commission found that the SFD had not yet reached its full potential and made several points for improvement. It invited Member States to:

- Implement fully the Swedish Initiative, including its principle of equivalent access.

In addition, the Commission indicated that it would:

- By December 2014, prepare for applying in this area the rules for ensuring national implementation of EU law.

The following sub-sections outline the developments in this area since the adoption of the EIXM Communication and the remaining gaps in order to shed light on the impact of the transposition and application of the SFD in daily practice. This will be done under the following sub-headings:

- Transposition of the Swedish Framework Decision;
- Operational compliance with the Swedish Framework Decision's legal requirements;
- Refusals to provide information on the basis of the Swedish Framework Decision; and
- Awareness of the Swedish Framework Decision and its perceived impacts.

4.1.1.1 Transposition of the Swedish Framework Decision

Two official reports have examined the implementation status and compliance with the SFD. In 2011, the application of the SFD was assessed by the Commission.[68] At that time, 16 Member States had transposed the Decision or informed the Commission that their national legislation was already in line with it.

The following year, the Danish Presidency issued a survey to Member States in order to further assess the extent to which national legislation complies with the Framework Decision's provisions. The relevant Council Report[69] indicates that by that time 22 Member States, as well as Liechtenstein, Norway, and Switzerland had transposed the provisions or had notified the Council that their national legislation was already in line with it[70]. The five exceptions were Belgium[71], Greece, Ireland, Italy and Luxembourg.

Based on the findings of this study, there has been some progress with regard to the transposition of the Decision since these reports. Greece adopted a presidential decree transposing the SFD in 2013[72] and Ireland has indicated that its national legislation is already in conformity with the SFD[73]. Belgium adopted implementing legislation on 25 May 2014. There are thus three Member States that are still to adopt implementing legislation, including Croatia that joined the EU in 2013. Interviewees from two of these Member States reported concrete plans for implementation. In Italy the matter is before Parliament. The police in Croatia were planning to start with implementation of the SFD in November 2014. The interviewees from Luxembourg had no plans for implementation to report.

The way the SFD has been transposed into national law in some Member States was criticised by a few policy makers and SPOC officers during the interviews. As a horizontal point relating to the transposition of the SFD in national law, some interviewees from these two groups noted that Member States have included the provisions of the SFD in several different national laws. This was regretted by these interviewees, who indicated that it would be clearer if the SFD could be found in one piece of national legislation or if an additional summarising decree (or similar) were adopted. We note, however, that this situation is not objectionable per se, as it is up to the Member States how to transpose EU legislation.

In addition, some interviewees noted that, in their opinion, not all aspects of the SFD are visible in the national laws, in particular relating to the principle of equivalent access and the time limits.

---

[68] *Commission Staff Working Paper on the operation of the Swedish Framework Decision,* SEC(2011) 593 (available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010316%202011%20INIT).

[69] *Council Framework Decision 2006/960/JHA – Assessment of compliance pursuant to Article 11(2), Council Report*, Council doc 14755/1/12 REV 1 (available at: http://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vj6iponbr3yj).

[70] Austria, Ireland, Malta, UK.

[71] Although the provisions were not yet fully transposed, Belgium reported to the Council that the Belgian police authorities already fully complied with the Swedish Framework Decision.

[72] Presidential decree 135/13.

[73] EIXM Communication, p. 8.

4.1.1.2 Operational compliance with the Swedish Framework Decision's legal requirements

Based on the research activities conducted for this study, the SFD is not yet applied as fully as it might be, as the previous reports have indicated.[74] In terms of the **use of and compliance with individual provisions**, this sub-section discusses:

- Use of the SFD forms;
- Compliance with time limits;
- Application of the principle of equivalent access;
- The extent to which information is shared with Europol; and
- The implications when judicial procedures are involved.

a) Use of the SFD forms

The **forms provided in the annex of the SFD are rarely used because they are not considered helpful**. This has already been raised by previous studies[75] and seems still to be the case based on the findings of this study. Indeed, most of our interviewees stated that they consider the forms to be time-consuming and labour-intensive without producing added value, since they are too detailed and difficult to use. Therefore, in most cases, requests are not sent using the SFD forms.[76] What is more, requests often do not refer to the SFD at all.

Interviewees from a few Member States noted that they use the form provided by SIENA for sending SFD requests. While there are not many Member States using **the SFD forms integrated in SIENA**, those who do so reported that this works rather well. SIENA provides support for easier filling in of the form, provides a certain validation of the content and a more automated way of dealing with the requests.

Based on a comparison of recent statistics provided by Europol to earlier statistics from the 2011 Commission's report on application of the SFD, there has been an increase in the use of SIENA for this purpose in recent years: a total of 653 SFD initiative requests were sent via SIENA in 2013, while 998 SFD initiative requests were received via SIENA. This can be compared to the figures provided in the 2011 Commission's report on application of the SFD, where it was indicated that the SFD form provided in SIENA has been used 56 times in 2009 and 51 times in 2010.[77] These numbers do not represent the total numbers of SFD requests, but only the requests sent *via SIENA*.

---

[74] These previous reports include: *Commission Staff Working Paper on the operation of the Swedish Framework Decision,* SEC(2011) 593; *Council Framework Decision 2006/960/JHA – Assessment of compliance pursuant to Article 11(2), Council Report***,** Council doc 14755/1/12 REV 1; the EIXM Communication; *Council conclusions following the Commission Communication on the EIXM*, Justice and Home Affairs Council meeting in Luxembourg, 6 and 7 June 2013 (http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/137402.pdf). The Council conclusions highlight in particular that there is room for improvement as concerns the implementation of the principle of equivalent access and the time limits.

[75] For example, the 2012 Council report stated that ten Member States indicated that they do not use the form at all. Others state that they prefer the form provided by SIENA. Some Member States did indicate that they use the forms for urgent requests or that they use form B, which they understand to be legally binding. We note that the SFD does not state that form B is legally binding. There are, however, situations in which the use of form A is legally binding (see for instance Article 4.4). The Commission's report on the application of the SFD similarly highlights that "only five Member States use the form annexed to the Framework Decision in order to request information."

[76] One interviewee pointed to a recent Dutch survey that came to the conclusion that the SFD limits rather than facilitates information exchange, mainly due to the cumbersome forms.

[77] *Commission Staff Working Paper on the operation of the Swedish Framework Decision,* SEC(2011) 593 (available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010316%202011%20INIT).

b) Compliance with time limits

The SFD's time limits are generally considered a positive feature. The time limits are kept to in most cases, but some Member States appear to be persistent laggards.

The Commission's report on application of the SFD states that **the time limits seemed to be complied with in most cases**.[78] This was also the general perception of the interviewees for this study. However, it was also reported during the fieldwork conducted for this study that there are sometimes cases where **responses are delayed**, sometimes by several months. Most interviewees who mentioned delays stressed that they do not happen often and in most cases occur with specific Member States. Indeed, it is the perception of our interviewees that some Member States are typically slower than others,[79] and there seems to have been no change in this regard in the past years. SPOC officers consulted regretted that response times are sometimes difficult to predict, as they generally seem to depend not only on the type of request, but also on the Member State. Where delays are typically associated with one Member State, this situation can lead to further delays, because **some officers base their efforts on reciprocity**. SPOCs are more inclined to provide quick responses to Member States that are usually also quick to reply and follow-up.

Apart from the propensity of certain Member States to be the source of delays, an important difficulty Member States struggle with is the limited number of SPOC staff. There has been **an increase in message exchanges, but not an increase in resources** in most Member States, as highlighted by our interviewees.[80] Staff shortages are one of the main reasons for delays.

Staff may also be under workload pressure from messages that are not strictly necessary. Some of the law enforcement managers interviewed felt that there is room to decrease the number of messages to increase efficiency, i.e. by aiming to restrict international correspondence to messages that are strictly necessary. Follow-up questions, e.g. asking when a response to a request can be expected, are generally not necessary but cause additional work for SPOC staff. In addition, our research showed that **"fishing" is sometimes used in SIENA,** i.e. sending a request for a cross-border check with a copy to all Member States. Such requests must be answered, which creates a need for resources that is not proportionate to the added value of the request.

Based on the input from a few interviewees, it is not clear whether the time limits are correctly reflected in all Member States' national laws or guidelines, which could be another reason for delays. For example, an interviewee from one Member State explained that the content of the SFD is reflected in three different national laws, but that the time limits are not explicitly mentioned. In another Member State a SPOC officer indicated that they have guidelines on response times, which are different from the SFD guidelines: non-urgent requests are to be responded to within one month, normal requests within ten days and urgent requests within 24 hours.[81] Based on the SFD-mandated

---

[78] The Commission received note from 26% of Member States that urgent requests have *always* been complied with. The majority of Member States, 62%, reported that the time limits for urgent requests are *often* complied with by their EU partners. There were also some Member States that "see compliance as a rare occurrence" (3%) or urgent requests can never be complied with (9%). *Commission Staff Working Paper on the operation of the Swedish Framework Decision,* SEC(2011) 593 (available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010316%202011%20INIT), *p. 9.*

[79] This was also highlighted by *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD (2010), (http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/icmpd_study_lea_infoex.pdf) p. 104.

[80] This was also noted in Council Document DS 1800/13, "*Answers to questionnaire on action 2 of IMS action list*", which indicates that "all Member States note an increase, with an average of 10% to 20% per year, of the incoming requests during the past ten years".

[81] *Commission Staff Working Paper on the operation of the Swedish Framework Decision,* p. 9: "All Member States have informed that they have legislative-based or practical procedures in place so that they can respond within at most eight hours to urgent requests for information and intelligence, in accordance with Article 4(1) of the Framework Decision."

time limits, urgent requests shall be responded to in eight hours, non-urgent cases shall be responded to within one week, and all other requests shall be responded to within 14 days. These issues were, however, only reported by individual interviewees. Irrespective of the time limits, most interviewees stated that they usually try to reply as quickly as possible.[82]

Technical differences can also lead to delays, as several interviewees highlighted. Achieving interoperability is still a challenge: our research showed that message content sometimes needs to be transferred manually from one programme to another because the channels used for international information exchange and internal messaging systems are not connected. In addition, an interviewee from the IT department of a law enforcement authority explained that there can be difficulties in cross-matching names, because diacritical marks are converted in different ways (e.g. a German "ü" could be written as "u" or "ue").

Another factor that may contribute to delays is connected to use of the "urgent" category. Some interviewees and participants in the expert panel in particular noted that there are **different interpretations of when a request deserves the designation "urgent"**. A few interviewees noted that the term is over-used because officers are afraid that their request will not be dealt with if it is not indicated that it is urgent. Therefore, the term is not taken seriously anymore. It was noted by a few interviewees that the reasons why a case is urgent are not always understood by the Member States receiving the request, e.g. because it is based on national procedural rules. Therefore, it was argued by these interviewees that delays could be avoided if officers always indicated why a request has been classified as "urgent".[83]

Finally, there is a general **concern whether time limits can be complied with when judicial authorities are involved**. This was raised by several interviewees from law enforcement services, during the expert panel and in our web-based survey.[84] The role of judicial procedures is further discussed at the end of this sub-section.

c) Application of the principle of equivalent access

Turning to the third area of concern, **the principle of equivalent access is implemented only to a limited extent**. In general terms, some interviewees indicated that there has been an improvement in this regard, while others noted that they had not observed any changes and that the principle is not yet applied. Several factors still seem to complicate the application of the principle.

First, there are several **general factors that hinder the full implementation of the principle of equivalent access**. In particular, the differences in the legal and administrative systems of the Member States and data protection legislation were mentioned in our web-based survey and during interviews.[85]

Second, the involvement of **judicial procedures** is also perceived to have implications for the implementation of the principle of equivalent access. The role of judicial procedures is further discussed at the end of this sub-section.

---

[82] Nevertheless, some interviewees indicated that they try harder with Member States that are responsive, as indicated above in this sub-section.

[83] This is in line with the earlier findings of the *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD (2010), p. 104.

[84] See also EIXM Communication, pp. 6-7.; *Council Framework Decision 2006/960/JHA – Assessment of compliance pursuant to Article 11(2), Council Report.*

[85] This confirms the findings of the *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD (2010), p. 8.

Another factor hindering equal access is the fact that there are **different crime prevention and combating priorities** among Member States, as well as different definitions of crime. Some requests are not replied to, as mentioned below, because the crime is not considered sufficiently serious in the Member State receiving the request.

Example of a typical case: different priorities

An EU citizen from Member State A was arrested in Member State B, because the authorities found 50 kg of hashish built into a motor home. The person was officially registered in Member State A, but habitually resident in Member State B. The regional criminal police in Member State A opened an investigation and consulted with the department on cannabis in the SPOC about how to proceed. The investigating officers clarified what type of information was needed. In this case, it was relevant to ask for vehicle registration data and the age of the person.

The SPOC then made a suggestion concerning the channel to be used. In similar cases, requests can be sent via the liaison officer. In this case however, the SPOC pointed out that the liaison officer in Member State B is very busy and that this case would not be considered a priority due to the low quantity of drugs involved. It was thus assumed that it would take too long to obtain the relevant information via the liaison officer. The SPOC thus suggested sending the request via a different channel, e.g. Interpol or Europol, because it expected that this might be faster. Even so, a response took three months, because the case was not considered a priority by the officers in Member State B.

Finally, during the interviews and in our web-based survey some policy makers and field officers indicated that the fact that **it is in many cases not possible to exchange information directly due to the role of the SPOCs** in the relevant Member States is a hindrance to the principle of equivalent access. The SFD does not specify the procedures according to which information should be obtained. Currently, direct exchanges are not always in line with national law. In some Member States it is obligatory to involve the SPOC in all international communication subject to very few exceptions. The interviewees argue that it should be possible for an investigator to contact the SPOC or competent authority[86] in another Member State directly, bypassing their own SPOC.[87]

While the interviewees appreciate the existence of the SPOCs, they regret that it is mandatory to involve them, because this is detrimental to ensuring that the distance between the source of the data and the end-user is as short as possible. Indeed, field officers prefer to be able to carry out some aspects of information exchange directly, rather than using the SPOC. This is reflected in field officers' comments in our web-based survey, pointing out that it would be desirable if procedures were shorter. Seven field officers responding to our web-based survey mentioned on their own initiative that direct access to SIENA would be desirable. This point is closely related to the role of SPOCs, which is further discussed in section 4.2.1. It can be noted in this regard that there is currently a movement towards more direct exchanges of information: some Member States have started or are planning to make SIENA available to officers in the field. This is further discussed in section 4.2.2.3.

[86] The idea was floated of creating an overview of all relevant authorities in the Member States to facilitate direct communication.

[87] Many field officers who participated in our WBS are of the opinion that it is **more cumbersome to obtain information from another Member State and that information is not in all cases supplied**. They explained that it usually takes longer to obtain the necessary information, in particular because the procedures and routes of communication involved are perceived to be lengthy and cumbersome.

d) Extent of information-sharing with Europol

Information sharing with Europol could be enhanced. Article 6(2) of the SFD includes an obligation to exchange information with Europol and Eurojust whenever an exchange relates to an offence within their mandate.

Based on Europol's statistics, there has been an increase in the information provided to it via the Europol Information System (EIS).[88] Yet, in general the extent to which information is shared with Europol was still not considered to be sufficient by previous studies[89]. Furthermore Member State contributions to the EIS and the Analysis Work Files (AWFs) vary per million inhabitants.[90]

Shortcomings in this regard have also been detected in the context of this study. Indeed, **not all field officers and SPOC officers are aware of the current possibilities or the fact that the SFD makes information sharing with Europol obligatory in some cases**[91]. This is one of the main reasons why there is not more sharing of information with Europol. Few departments in the Member States seem to have concrete instructions about when and how information should be shared with their ENU or with Europol directly. Usually, it is left to the ENUs to take any necessary steps. Many officers who participated in our web-based survey do not actually know of the EIS. Only a few officers indicated that they know of additional possibilities for sharing information with Europol and specified these.

Another reason for the limited extent of information sharing with Europol mentioned by some of the interviewees relates to reservations about sharing sensitive data. Some officers will **not upload very sensitive data to the EIS if they feel this will endanger ongoing investigations**.[92]

In addition, entering data into Europol's databases is seen as too time-consuming. One interviewee pointed out that it is in particular **difficult to guarantee the respect for the EIS data protection clauses in a small operational department**. Data uploaded to the EIS needs to be checked at regular intervals. According to this interviewee, these intervals are rather short, which is why too many resources would be required.

e) The implications when judicial procedures are involved

As indicated above, **judicial procedures are seen as time consuming** by many of the stakeholders consulted. In particular, they are perceived to render the time limits of the SFD ineffective and hinder the principle of equivalent access, which also has implications for Prüm follow-up requests (cf. section 4.1.2.2)

According to several stakeholders consulted for this study, the difficulties arise where the national laws of some Member States define the information to be shared between law enforcement authorities as

---

[88] *Europol Review 2012,* p. 27. *Europol Review 2013, p. 18.*

[89] *Commission Impact Assessment on adapting the European police Office's legal framework with the Lisbon Treaty,* pp. 8ff. *(http://www.ipex.eu/IPEXL-WEB/dossier/document/SWD20130098.do)*; *Study on the implementation of the Europol Council Decision, RAND Europe 2012,* p. 47 (https://www.europol.europa.eu/sites/default/files/publications/rand_evaluation_report.pdf); *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD (2010) (http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/icmpd_study_lea_infoex.pdf).

[90] *Commission Impact Assessment on adapting the European police Office's legal framework with the Lisbon Treaty,* pp. 8ff. *(http://www.ipex.eu/IPEXL-WEB/dossier/document/SWD20130098.do)*

[91] This was also raised in the *Study on the implementation of the Europol Council Decision,* RAND Europe 2012, (p. 50, pp. 55ff), op. cit.

[92] This was also raised in the *Study on the implementation of the Europol Council Decision,* RAND Europe 2012, (p. 50, pp. 55ff), op. cit.

judicial and not police information.[93] This distinction has practical implications: for example, an expert panel participant explained that the SFD cases have a life cycle which starts with investigation and ends up in prosecution/court. The SFD was put in place to obtain information for the purpose of investigations. For data used at the prosecution stage, it is common for the rules on judicial cooperation to be relevant, including e.g. the need for a MLA.[94] For the investigation part, the need for judicial assistance and letters rogatory slow down exchanges and is not necessary according to this expert panel participant and several interviewees. However, interviewees and expert panel participants underlined that this was only relevant with regard to certain countries. These include the Benelux countries in particular, but Lithuania and others were also mentioned.

Although this point was raised by many of the interviewees and has concrete practical consequences, the requirement for judicial involvement in information exchange at the investigation stage is **in line with the principle of equivalent access as long as the same formalities apply to internal information exchange**. The problem thus seems to be mainly rooted in differences in national legal systems. These are beyond the scope of this study.

The recent adoption of the Directive on the European Investigation Order[95] is expected to influence law enforcement information exchange positively in the future,[96] as it facilitates Member States in obtaining the evidence needed in the context of criminal proceedings from another Member State. A European Investigation Order may be issued in order to institute investigative measures but also to obtain evidence that is already in the possession of the competent authority. It was pointed out during the expert panel that with the European Investigation Order, judicial cooperation is now moving ahead faster than police cooperation and the former is expected to bring flow-on benefits to the latter.

4.1.1.3 Refusals to provide information on the basis of the Swedish Framework Decision

There is no comprehensive overview of refusals on the basis of the SFD. Based on the research activities conducted for this study**, refusals are an exception**[97].

Five years ago it was estimated that between 75% and 100% of the requested information or criminal intelligence were obtained. If the requested data could not be provided, reasons were given in almost all cases. Cases where Member States did not reply at all were very rare.[98]

Based on the research activities carried out for this study, these estimates still seem to be accurate. In our web-based survey, we asked the SPOC officers to specify the relevance of individual reasons for refusing requests. The majority stated that the reasons suggested as part of the question[99] were not

---

[93] This was also highlighted by the Council report *Council Framework Decision 2006/960/JHA – Assessment of compliance pursuant to Article 11(2), Council Report***,** Council doc 14755/1/12 REV 1 (available at: http://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vj6iponbr3yj).

[94] Cf. also EIXM Communication, pp. 6-7.

[95] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.130.01.0001.01.ENG).

[96] Member States must comply with the Directive by 22 May 2017.

[97] See e.g. *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD (2010), pp. 46 ff.

[98] *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD 2010 (http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/icmpd_study_lea_infoex.pdf)**.**

[99]The following were given: Providing it would harm essential national security interests of the requested Member State; Providing it would jeopardise the success of a current investigation or a criminal intelligence operation or the safety of individuals; Providing it would clearly be disproportionate or irrelevant with regard to the purposes for which it has been requested; The request relates to an offence punishable in the requested Member State by a term of imprisonment of one year or less; The competent judicial authority in the requested Member State did not authorised the access and exchange

relevant ("never used as a reason") or that they did not know whether they were relevant, implying that requests are not often refused. Indeed, many interviewees indicated that they experienced refusals only rarely, if at all.

Based on the different research activities carried out in the context of this study, **different reasons seem to be relevant for refusing information**:

- Based on our web-based survey, **the reasons mentioned in Article 10 SFD** seem to be used to some extent but not often.[100]
- Some respondents to our web-based survey and interviewees stated that requests are sometimes **refused because a letter rogatory is required and the request has not been addressed to the judicial authority**. We note here that this would be in breach of the SFD. Based on Article 3.3 of SFD, it should only be possible to request a letter rogatory, if this is also required for internal requests. If this is the case, the requested authority should forward the request to the relevant judicial authority instead of refusing it.[101]
- Another reason mentioned by several interviewees is the fact that the relevant act was **not considered sufficiently serious (or not considered a crime)** in the other Member State. For example, driving without a driving licence is defined as a crime in Romania, but not in Hungary (where it is a motoring offence). Other Member States have a certain minimum financial value that needs to apply in order for a case to be prioritised or be considered at all relevant for cross-border information exchange.
- Specifically for PCCCs, the reasons for refusing such requests could be related to the **competencies of the PCCC** (e.g. they are not competent to deal with requests related to terrorism).

4.1.1.4 Awareness of the Swedish Framework Decision and its perceived impacts

The picture of awareness of the SFD is mixed, while in general **awareness of the instrument is limited**. There is a difference between field officers and SPOC officers in the expected and actual level of awareness.

Field officers are not, in general, aware of the SFD, nor of the legislation and procedures. **Nor may it be necessary for them to know about the SFD**. Some of the stakeholders consulted argue that for most police officers, international information exchange is an exception[102]. On this basis, some participants in the expert panel voiced the opinion that field officers do not need knowledge about the different instruments at EU level. They (or their superiors) do need to have a broad overview of the types of information that might be interesting to share and they need to know that they can contact the SPOC when relevant.[103]

While it may indeed not be necessary for field officers to know about the technicalities of using a specific channel if the SPOC handles this, we underline that field officers do need to know about the existence of the national SPOC, and when and how it should be contacted. In addition, in-depth

---

of the information requested; Refused for other reasons (please specify); I never had a case of either receiving or sending a refusal.

[100] There were only a few respondents who indicated that any of the reasons is often used as a reason to refuse requests.

[101] See also section 4.3.2 on *Further general considerations*.

[102] We note, however, that the number of correspondences is generally increasing, as pointed out by different stakeholders.

[103] Depending on the national structures, this might not even be necessary. When information is registered in central data bases, the analysts at the SPOC could determine when there is a piece of information that might be connected to a cross-border case.

knowledge is necessary in some Member States where field officer involvement is more direct (e.g. when SIENA is used in the field). This view was confirmed by several interviewees.

In practice, there is currently a **lack of awareness among field officers and investigators of the benefits and use of international information exchange**. While field officers generally know that it is possible to make a request of other Member States, it is debatable whether they are really aware of all the cases where they can actually ask for information from other countries. This means that they do not contact the SPOC for cases where they should. This was, for example, raised by interviewees from Sweden, who indicated that the number of requests from field officers to the Swedish SPOC had been too low. So the Swedish SPOC developed a workshop for field officers, which helped to increase the volume. This is described further in section 4.3.1.1.

There is also a **lack of awareness of the procedures** involved, which can lead to delays. For example, according to the experiences of an officer in a 24/7 unit in a SPOC, around half the time field officers call before submitting a request that relates to a new case to make sure that they are using the correct procedure.

Although the SFD as a legal basis may be rather abstract, national instructions outlining the procedures in a more accessible way can be helpful in supporting field officers. However, **there are no up-to-date national instructions on the procedures related to information exchange in all Member States**. Some Member States seem to have instructions that are not known about or used by the desk officers. Indeed, for some Member States policy makers and field officers/SPOC officers gave conflicting accounts during interviews and the web-based survey of whether or not general instructions exist, suggesting that desk officers are not always aware of existing instructions. In other Member States guidelines exist but are not updated regularly, so there is no practical relevance. Some SPOC officers explained that the legal texts and any updates that are circulated are the most relevant sources of information.

Where they do exist, instructions normally outline the internal routes of communication. In some but not all Member States[104], they state when and how international correspondence should be initiated. In our web-based survey, close to two thirds (28) of the policy makers indicated that the SFD is taken into account in the instructions, whereas most others did not know.

SPOC officers have by nature a better overview of the SFD and the procedures involved than field officers.

However, even among SPOC officers there seems to be some **confusion about the concepts related to the SFD**. For example, quite a few interviewees indicated that they still use Article 39 CISA[105]. This was confirmed during an interview with a manager at a law enforcement authority and the expert panel. Another hint of confusion is the fact that different interviewees at national level gave different accounts of whether and how the SFD is applied in that Member State in practice. In addition, the SFD for many only relates to the forms. This also demonstrates an information gap. Indeed, when asked

[104] In the web-based survey, respondents from a few Member States indicated that instructions do *not* include information on how to act when confronted with a cross-border case. This is an interesting finding, as the purpose of the manuals should be to provide information on cross-border cases and it might be expected that the most relevant information for field officers would relate to the question of how to act. Unfortunately it was not specified in the web-based survey what the instructions cover if guidance on how to act is not included.

[105] Convention of 19.06.1990 implementing the Schengen Agreement (CISA), OJ 2000 L 239. Article 39 requires police authorities to assist each other and thus established the main legal basis for exchange of information between the police authorities of the Schengen States [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:42000A0922(02)].

about the application of the SFD, many interviewees only pointed to the forms. Only a few interviewees recognised that the SFD is the legal basis that facilitates information exchange.

The practical impact of the SFD is generally perceived to be limited. This was confirmed by some of the interviewees and participants in the expert panel. This is not in contradiction with the fact that the SFD in itself is **a horizontal principle more than a practical instrument**. Indeed, it was never meant to be 'used' as a tool. The forms were not envisaged in the original proposal. **This said, the general conclusion of the fieldwork conducted for this study is that it has only been possible partially to achieve the expected benefits of the SFD[106] and that the benefits of the SFD are not always recognised as such by practitioners**.

Some of the interviewees did nevertheless highlight some benefits that they feel the SFD has brought. For example, a few interviewees pointed out that the SFD made information exchange compulsory unlike Article 39 CISA. In addition, some interviewees considered it very positive that the SFD does include procedures and time limits, unlike Article 39 CISA. The general perception among policy makers seems to be that the idea behind the SFD is still valid: availability of information based on indiscriminate and timely access. Yet, many SPOC officers interviewed indicated that the SFD does not have any practical relevance for them.

A possible reason for the perceived limited relevance of the SFD is the fact that many interviewees associate the SFD only with the forms, as pointed out above. This is the conclusion of the study team, based on the fact that many interviewees only referred to the forms when asked about the relevance of the SFD. Indeed, some interviewees saw the forms as the main novelty of the SFD; they were of the opinion that the other aspects, such as the time limits, predated the SFD. Others argued that they *do not use the SFD at all*. When asked to explain this statement, the interviewees argued that they do not regard *the forms* as useful and thus do not use them. This argumentation suggests that the SFD is not recognised as a legal basis, but is only associated with the forms. The perception that the SFD does not have practical relevance could also be related to the fact that generally no reference is made to the SFD in requests and that no channel is specifically designated to it or associated with it. Thus, officers generally use the SFD as a legal basis without being specifically aware of this fact.

4.1.1.5 Conclusions

There has been progress in the implementation of the Swedish Framework Decision: most Member States have transposed it. However, it is still not being applied as fully as it could be.

In particular, the forms are rarely used because they are considered too cumbersome. Consequently, it is normally not indicated that a request is based on the SFD unless the form provided in SIENA is used. This is, however, not yet the case in many Member States.

The time limits are considered useful and are complied with in most cases. However, delays still occur. The reasons include insufficient resources to handle an increased volume of information exchange, e.g. including messages that are not strictly relevant. In addition, there is no common definition of the term "urgent" and often no reasons are stated why messages are classified as "urgent".

---

[106] This is in line with the findings of previous reports, including: *Commission Staff Working Paper on the operation of the Swedish Framework Decision,* SEC(2011) 593 (available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010316%202011%20INIT)*; Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD 2010 (http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/icmpd_study_lea_infoex.pdf)*, Council Framework Decision 2006/960/JHA – Assessment of compliance pursuant to Article 11(2), Council Report***,** Council doc 14755/1/12 REV 1 (available at: http://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vj6iponbr3yj).

There are also impediments to the principle of equivalent access. In general terms, differences between legal and administrative systems of the Member States complicate the application of the principle. The obligatory involvement of SPOCs in some Member States can be seen as hindering the principle of equivalent access, because the distance between the source and end-user of information is extended. Different priorities in relation to what types of crime are worth pursuing are another factor that can prevent successful information exchange. This point is closely related to the lack of resources.

Information is not shared sufficiently with Europol, in particular because there is a lack of knowledge of the obligation to do so and the means that could be used. In many departments, there are no clear instructions on when information should be shared with Europol.

The involvement of judicial authorities is perceived by the representatives of law enforcement authorities interviewed as delaying information exchange and thus weakening the principle of equivalent access and rendering time limits ineffective. While this is a concern to many of the stakeholders consulted, the differences in national legal systems are beyond the scope of this study.

On a positive note, there are seldom refusals to provide information. When requests are refused, this is often due to the fact that letters rogatory are required but the request was addressed to the wrong authority. This is not in line with the SFD, which requires that a request addressed to the wrong authority be forwarded.

Another factor hampering the application of the SFD is the fact that SPOC officers and field officers' awareness of it is limited. Field officers are not sufficiently aware of the procedures related to information exchange, including when and how to initiate exchanges. In addition, there is some confusion about the SFD among SPOC officers. In particular, the SFD is mostly associated with the forms. In addition, quite a few interviewees indicated that they still use Article 39 CISA. On this basis, the practical impact of the Swedish Framework Decision (SFD) is perceived to be limited by most stakeholders consulted.

The SFD is a horizontal principle, not a practical tool. In fact, however, many operational officers consider the SFD forms as its main novelty and argued that the other aspects, such as the time limits, were already applied before the adoption of the SFD. That the forms are not used means for some that the SFD as such is not used.

4.1.1.6 Recommendations

Based on the findings of this study, it seems that the general principles of the SFD, in particular availability of information based on indiscriminate and timely access, should be promoted further and its use in practice be encouraged. It is considered that the following activities would be useful in this regard:

- The SFD needs to be fully reflected in national law, including in particular the principle of equivalent access and the time limits. It would be appropriate to analyse further the progress of Member States in implementation of the SFD and consider relevant actions in the light of the changed competences of the Commission in December 2014.
- There seems to be a strong need for increased awareness-raising of policy makers and operational users of the SFD on its principles, including information-sharing with Europol. Consideration should be given to reviewing the EU guidelines on the use of the SFD where necessary. These guidelines could be part of a larger project, such as the Information

Exchange Platform (IXP) or the Infopolex Initiative.[107] It would be necessary that the guidelines be made available to law enforcement officers in their own language. It is considered that it would be useful to include the following specific points in such guidelines:

- Article 39 CISA has been replaced by the use of SFD for matters within its scope;
- Simplified overview of the SFD's purpose and main principles;
- Overview of the relevant data protection principles that apply to exchanges under the SFD;
- Prioritising in relation to urgency and how to justify why a request is considered urgent;
- Requests that are directed to the wrong authority should not be refused but forwarded; and
- Only strictly necessary messages should be sent to ensure efficiency.

- To further enhance the SFD's practical use, practical mechanisms of how to implement SFD principles in daily business should be developed, such as facilitating the use of SIENA for SFD requests.

- A possible amendment of the legislative instrument should be examined. Consideration should be given to:
  - Defining a channel for sending SFD requests and referring to the role of the SPOCs; and
  - Abolishing the forms and pointing to the form integrated in SIENA, depending on the extent to which SIENA is used by then (cf. section 4.2.2.3 and 4.2.2.4).

[107] The Information Exchange Platform has been developed by Europol and presented to the DAPIX working group. The proposal includes developing a common portal with help functions, guidelines and also an operational multi-query function for all relevant EU systems. The Information Exchange Platform is discussed in section 4.2.2.4 *Feasibility of standardisation of the use of the different channels and SIENA*. The Infopolex Coordination Initiative which was presented to the DAPIX working group, too, is a project led by Hungary. It aims to prepare common standards and guidelines for the area of information exchange.

4.1.2 Implementation and operational compliance with the Prüm Decisions

As explained under section 3.3.2, the Prüm Decisions were put in place to step up cross-border police cooperation, in particular by allowing for automated search of data, supply of data in relation to major events, and supply of information in order to prevent terrorist offences. In the EIXM Communication the Commission found that the Prüm Decisions are not yet fully implemented in all Member States and that they are not applied consistently.

In line with the above, the 2012 EIXM Communication invited Member States to:

- Implement fully the Prüm Decision, using the EU support available;
- For Prüm post-hit follow-up requests, to use the SFD and SIENA; and
- Improve Prüm statistics.

The Commission was to:

- Continue to provide EU funding to support implementation of Prüm; and
- By December 2014: prepare for applying in this area the rules for ensuring national implementation of EU law.

4.1.2.1 Implementation of the Prüm Decisions

The state of the implementation of the provisions of the Prüm Decisions was analysed in a 2012 Commission Report.[108] This document highlighted that the Prüm Decisions should have been fully implemented until August 2011, but Member States were lagging behind with regard to the transposition of provisions related to DNA data, fingerprints, vehicle registration data, national contact points, and data protection.[109]

In the same year, 2012, a Prüm helpdesk had been established at Europol in order to support the Member States in implementing and applying the Prüm Council Decision.[110] However, the implementation report noted the low use by the Member States' authorities of the Europol helpdesk, as well as of the relevant funding instruments, and the targeted support offered at that time by the Mobile Competence Team (MCT)[111].

---

[108] Report from the Commission to the European Parliament and the Council on the implementation of 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 (the 'Prüm Decision'), COM(2012)732, c.f.: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0732:FIN:EN:PDF.

[109] The report looked into technical issues and funding as reasons for implementation delays, but nevertheless indicated that "[g]iven the various possibilities to obtain support and the long period of time that has elapsed since the adoption of the two Prüm Decisions, it is hard to see any reasons which could justify lack of implementation. What is needed above all seems to be political will and appropriate prioritisation to overcome barriers at national level."

[110] Support is offered in particular in the following areas:

- Technical support to implement the Prüm Decisions;
- Support for States in their daily fingerprint and DNA information exchange mechanisms; and technical support with regard to further development of the network.

[111] MCT was a Commission-funded German project aimed at supporting non-operational Member States in implementing the Prüm Decisions. The MCT was established on the basis of an ISEC-funded project, which ended in July 2014, with its tasks being taken over by the Europol helpdesk. C.f. http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/mct_en.htm.

Two years after the publication of the Prüm implementation report, we observe that the **implementation** of the Prüm decision is **still not up to speed**. This is demonstrated by the slow evolution in this period shown in the table below.

Table 3: Evolution of Prüm implementation (2012-2014)

Type of data	Number of Member States implementing as of December 2012	Number of Member States implementing as of November 2014
DNA data	18	20
Fingerprint data	14	17
Vehicle registration data	13	19

Sources: Prüm implementation report (2012), information communicated by Europol to the study team (2014)

Assessing the latest table on the state of play of Prüm implementation by the Council[112], we observe that there are seven Member States that are not yet operational for any of the three types of Prüm data (Croatia, Denmark, Greece, Ireland, Italy, Portugal and United Kingdom) and hence have not yet connected with any other Member State.

As a possible reason for the delay in Prüm implementation, some interviewees indicated that Member States start by connecting with one or two neighbouring countries but, as the costs for establishing connections are significant, they do not continue investing in creating connections with Member States further afield in order to extend their Prüm usage to all operational Member States. It seems that Member States do not feel there is binding obligation to interconnect completely, and Member States' reluctance actually also effects their counterparts' abilities to expand their connections ('negative peer pressure').[113]

In addition, increasing volumes of data are being exchanged under Prüm (and in general for SPOCS, as flagged under section 4.3.2.3) due to the establishment of new connections among existing members and with the accession of new Member States to the EU. At the same time, national budgets devoted to international police cooperation have not been increasing.

In line with the Prüm implementation report, our expert panel participants pointed to **lack of focus and political will** as determining factors in the slow implementation of Prüm by the Member States.

A further issue with implementation seems to be the fact that DNA and fingerprint hits[114] both have to be **verified**[115], which necessitates resources. Some interviewees felt that this has actually not been sufficiently taken into account when considering Prüm expansion.

---

[112] *Implementation of the provisions on the information exchange of the Prüm Decisions*, 5124/5/14 REV5, JAI 7, DAPIX 1, ENFOPOL 1, CRIMORG 2, 17 September 2014.

[113] We refer here to the point raised under the section 4.1.1.2 *Operational compliance with the Swedish Framework Decision's legal* requirements, where some interviewees highlighted that they view information exchange as a matter of reciprocity.

[114] While direct access is provided by Prüm to Member States' vehicle data, fingerprint and DNA can only be accessed via follow-up procedures based on a hit notification.

[115] We note in this respect that in the case of *S. and Marper v. the United Kingdom* (http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-90051#{"itemid":["001-90051"]}), the European Court of

Last, but not least, expert panel participants were of the opinion that the **purpose of Prüm is actually not entirely clear** as at present it is used both for systematic checks (i.e. "fishing for matches") and targeted case-by-case comparisons of profiles. Not having an agreed exact purpose results in uncertainties about quality requirements for matching rules, as well as the ideal IT architecture.

4.1.2.2 Follow-up of hits

The automated search function of Prüm was already highlighted by the 2012 Prüm implementation report as a major benefit, and this was also the perception of our interviewees, as it provides immediate feedback on requests. This makes it possible to know where information is available. However, proper follow-up of DNA and fingerprint hits is essential in order to provide information that is actually useful for investigators.

The 2012 Prüm implementation report already noted the **heterogeneous picture** concerning **the tools used to follow up Prüm hits**. Based on a specific questionnaire conducted for the report, the Commission observed that at that time, the Europol and Interpol channels were used by Member States to roughly the same extent for follow-up requests. Only a few Member States preferred the SIRENE offices or bilateral liaison officers.

Our interviews, as well as our web-based survey results[116] indicate that **currently Member States mostly seem to use the Interpol channel for Prüm follow-up**, followed by SIRENE and SIENA This is a recognisable difference from two years ago, and notable in light of the fact that the EIXM Communication recommends that SIENA be the default channel for follow-ups.

Interpol seems to be used to some extent in all Member States according to the web-based survey, and the share of respondents that indicated that they never use this channel is lower for all Member States compared to the other two channels. The most frequent response on SIENA was "I never use it". In fact, SIENA is used to a large extent for Prüm follow-only in some Member States. On the other hand, a high number of respondents indicated that they never or hardly ever use SIENA.

It is important to note that while there are national preferences regarding the channel to use for the follow-up, **significantly different approaches seem to exist also *within* the Member States,** with different answer categories being chosen by our web-based survey respondents from the same given Member State. On the other hand, some Member States had a rather equal spread of the different answer alternatives.

Instructions on the Prüm follow-up channel are not always in place in the Member States. In most countries, it is possible to use different channels. Only a few respondents to our web-based survey indicated that they only use one specific channel, implying that most officers are somewhat flexible in their approach. In fact, based on our interviews, we note that in some SPOCs a certain section is not always aware of another's Prüm activities. Based on our interviews and expert panel, we observe

Human Rights concluded that in that case regarding persons who had been suspected but not convicted of an offence, […] the blanket and indiscriminate nature of the powers of retention had failed to strike a fair balance between the competing public and private interests, and the United Kingdom had overstepped any acceptable margin of appreciation in that regard. Furthermore in the *S. and Marper* case, the Court noted that the retention in question constituted a disproportionate interference with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society.

[116] For a more detailed view on respondents input on this and other aspects, c.f. Annex 1.

furthermore that national preferences for follow-up channels seem to actually stem from mid-management's choices and/or be based on operators' convenience or simply habit.

While numerous stakeholders argue that it is necessary for the continuity of the exchanges that the choice of channel be open, we note that SPOC personnel currently have to deal with a complex matrix of national preferences for follow-up channels with the different Member States. Hence our findings based on our interviews reaffirm the Prüm implementation report's observation that **the diversity of follow-up channels can indeed lead to delays** in information exchange.

As mentioned in section 4.1.1.2, there is a general concern on whether time limits can be complied with when judicial authorities are involved. The final report of the Commission's mapping exercise[117] noted that where Member States' legal and procedural regimes differentiate between information obtained by police and by judicial authorities, this can present problems. Depending on the country, Member States may ask for a given type of information through police co-operation channels if it is considered a police issue in the destination country, while in other countries it may be considered judicial information to be exchanged only through a request for mutual legal assistance. Our interviews suggest that the need for is MLAs still an issue in some Member States (e.g. Belgium and the Netherlands seems to require MLAs to obtain the name of a suspect following a hit).[118]

In order to facilitate the use of SIENA (as the recommended default channel for Prüm follow-up) Europol has developed a **UMF Prüm Hit Follow-up Form** that can be attached to SIENA messages. However, the use of this form is reported[119] to be still rather limited. Austria, Cyprus, Czech Republic, Lithuania, Romania and Slovenia are using the form, although not on a regular basis and mostly only for simple cases. The extent to which the form is used of course is fundamentally affected by the relatively low rate of utilisation of SIENA as the preferred communication channel for the Prüm follow-up process. The practical obstacles to using the form, which have been identified by the Member States and were communicated to the study team by Europol, relate mainly to the form's complexity, file size (for complex cases, with attachments) and technical incompatibility with national systems. Europol is currently looking into these issues and trying to find a way to make the form more "user friendly".

Using the SFD for Prüm follow-up was only mentioned by few interviewees, who noted this possibility. However, as mentioned in section 4.1.1, based on our interviews we observe that the SFD is referred to as the legal basis for a request on only a very few occasions. In most cases, it is not (while being regarded by some as implicit). Some of our expert panel participants argued that there is no need for such specifics or mention of legislation in the follow-up procedures because it is understood that they are covered under the SFD.

4.1.2.3 The absence of reliable statistics and the impact of Prüm

The 2012 Commission Report on Prüm reiterated the importance of relevant statistics in assessing assess the added value of the Prüm Decisions. However, our study team found that statistics of Prüm hits that were followed up and used in investigations are in practice still not available. Several interviewees noted that the statistics were not sufficiently developed to allow conclusions to be drawn on the actual impact of Prüm on investigations.

[117] Confidential report.
[118] However, ensuring proper judicial cooperation complementary to the Prüm cooperation seems to be an issue for Member States where biometric data are handled by judicial authorities.
[119] Communication from Europol.

Another reason for the lack of statistics is the complexity of the procedure. The data on the number of hits is not comprehensive. Hits need to be verified. Those which will indeed be verified are only an unknown subset of the overall hit count. Another point of reference which it could be interesting to look at once the exchange is completed is the number of cases in which information obtained following a hit was actually used in a judiciary procedure. However, the further one looks into this process, the less likely it is that reliable quantitative data can be found.

Hence we note that while the number of Prüm hits is interesting, data which would be more relevant (and more difficult to obtain) would be the extent to which the data obtained via follow-ups were actually used in the investigation or in court. While we were not able to obtain any data on this, one interviewee did estimate that around 70% of hits are distributed to the police for follow-up and in the end only about 5% are really used in legal proceedings. The same interviewee judged this to be a satisfying end- result as the cases concerned are the more serious crimes.[120]

While monitoring the actual outcome of Prüm exchanges in judiciary proceedings is very challenging due to the issues mentioned above, statistics on the actual number of hits that were followed up at all in investigations (irrespective of the specific impact on judiciary proceedings) seem in principle to be easier to produce. However, as there is no designated channel for Prüm follow-up, Member States in fact encounter some challenges themselves in producing statistics since (as demonstrated above), the choice of channel varies even within the same Member State.

The impact and utility of Prüm are also believed to depend on the **matching rules.** According to the Prüm implementation report, these were considered by a significant number of Member States to be not fully satisfactory, in particular for DNA data. Matches can occur that are found to be false upon subsequent verification. The question of quality standards for fingerprint markers was also raised by our expert panel participants.

4.1.2.4 Conclusions

Due to lack of prioritisation in several Member States, the implementation of the Prüm Decisions is still lagging behind the ambitions for it. It is highlighted that a Prüm helpdesk was established at Europol in order to support the Member States in relation to the implementation and application of the Prüm Council Decision.

Procedures for following up on Prüm hits are not clearly defined in the Member States. There is currently also an ambiguity among practitioners about whether the SFD should be used for Prüm follow-up or not.

Interpol seems to be the channel that is used most frequently for Prüm follow-up, but most officers use different channels which depend on the specific case.

The diversity of follow-up channels can lead to delays in information exchange due to duplication of work or risk of coordination mistakes.

Statistics on Prüm hits that were followed up and used in investigations are not available as the current data gathering does not reflect the complexity of the Prüm process.

[120] We note here that often Prüm is used together with other investigatory steps without being strictly referred to.

4.1.2.5 Recommendations

The progress of Member States in the implementation of the Prüm Decisions should be analysed further and adequate action should be taken in order to ensure compliance with the current (expired) implementation deadline.

Furthermore, we recommend the setting up of and agreement on individual roadmaps per delayed Member State for the **implementation of Prüm**, including:

- A deadline by which a Member States must have implemented each category of data exchange with at least one other Member State; and
- A deadline for full implementation, i.e. for connecting to all other Member States for all categories of data.

A central support facility including a Prüm helpdesk function should be strengthened. It should be determined which institution (eu-LISA, Europol) is best placed to do what type of activity in this regard.

In terms of the **Prüm follow-up** process:

- Data of Prüm hit follow-up exchanges with Europol/EIS should be shared with Europol, since Prüm hits automatically establish the relevance of this data for the agency.
- It should be clarified that SFD should be used for the follow-up process.

With a view to allowing a more targeted search and minimising the number of validation checks yielding a negative result, defining clearer DNA and fingerprint matching rules should be considered.

The full expansion potential of Prüm exchanges should be analysed, and the consequences in terms of actual and expected volumes of exchange requests, as well as resources needed should be monitored.

Fine-tuning the purpose of Prüm exchange by defining whether the goal is exchange on an operational case-by-case basis or blanket checks should be considered.

The utility and feasibility of moving away from a hit/no-hit system to direct access for fingerprint data should be looked into. Any such move should fully respect the principle of purpose limitation and the data protection limits on storing DNA data established by the European Court of Human Rights[121].

[121] C.f. case of *S. and Marper v. the United Kingdom* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-90051.

4.2 Processes and practical aspects of information exchange

In this section we discuss the practical aspects of information exchange, including key operational features and players in implementation of EIXM in practice.

4.2.1 The Single Points of Contact (SPOCs)

The 2008 Manual of Good Practices concerning the International Police Cooperation Units at National Level[122] underlined the advantages of setting-up a "one stop shop" unit for international police cooperation, with a multi-agency organisation within each Member State. The Manual emphasised that setting up such a unit was a matter of national competence, which had to take account of each Member State's legal situation and law enforcement structures. Nonetheless, it stressed the advantages stemming from adopting such a set of recommendations and the general efficiency of EU police cooperation exchange as a whole.

The purpose of this institution is to make cross-border police cooperation more effective by subsuming into it the competencies of different national offices or contact points. These involve:

- The Europol National Unit (ENU);
- The Interpol National Central Bureau (NCB);
- The SIRENE Bureau;
- The contact point for national liaison officers posted abroad and foreign liaison officers posted in the Member State;
- The contact points designated pursuant to the "Swedish Framework Decision" and the "Prüm Decisions" (step 2 – exchange of additional information following a hit for DNA, fingerprints and VRD); and
- If any: the contact point for the regional and bilateral offices.

With respect to the SPOC concept, the 2012 EIXM Communication invited Member States to:

- Create, if not already existing, a Single Point of Contact (SPOC) covering all main channels, available 24/7, bringing together all law enforcement authorities, with access to national databases.
- Ensure that information exchanged through Police and Customs Cooperation Centres is where appropriate passed up to national level, and where relevant to Europol.
- Establish cooperation between SPOCs and EUROSUR[123] NCCs[124].

[122] C.f. http://register.consilium.europa.eu/pdf/en/08/st07/st07968.en08.pdf.
[123] European Border Surveillance System.
[124] National Contact Centres.

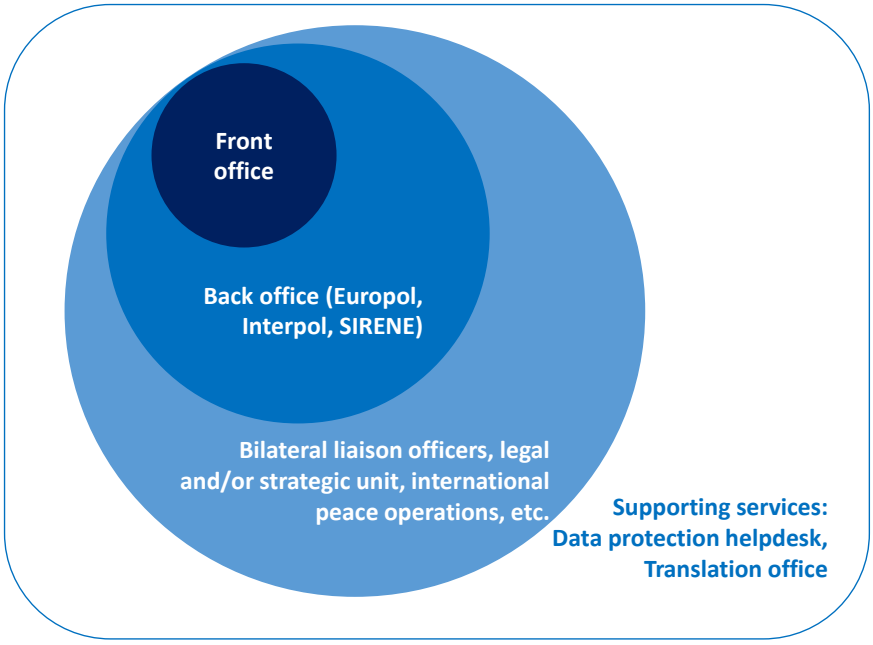
4.2.1.1 Application of the Single Point of Contact concept in the Member States

In June 2014, the Council adopted the SPOC Guidelines for international law enforcement information exchange, which for the most part[125] reused the material of the 2008 Manual discussed above. As a new element, a section was added on the SPOCs' case management system, which defines a "circle of criminal intelligence" (receipt-evaluation-distribution) and provides a proposed classification of urgency.

The vast majority of Member States have an international police cooperation structure that at least partly complies with the criteria set by the EIXM Communication and the subsequent SPOC Guidelines. At the same time, many national systems are currently under review and in a process of transformation.

A detailed distinction among and typology of the different versions of SPOCs is in fact made redundant by the different national ways of working and the different institutional set-ups in the Member States. The understanding of which level of the relevant structure actually qualifies as a SPOC seems very different. Some interviewees understand as 'SPOC' only the front office (or 'communication centre'); for others, it means the entity housing the three channels (Europol, Interpol and SIRENE) together[126]. The definition of yet another set of interviewees has the largest scope, in which in addition to all these elements the SPOC also contains further strategic and support services[127]. The basis scheme of these levels (or layers) is presented in the Figure below.

Figure 2: The different layers of a SPOC



Source: Deloitte

Some Member States do not yet have a SPOC at all.

[125] References in the Manual to "international police cooperation unit" were changed to SPOC, and instead of good practices the new document refers to guidelines.
[126] In some Member States there are thematic divisions in the back office, e.g. on crimes relating to property, drugs.
[127] NB in Austria and Germany the complete central criminal police (including the thematic divisions that would coordinate the work on concrete cases relating to international exchanges) is in theory understood as being the SPOC.

Case example: establishment of a SPOC

Greece is currently in the process of setting up a SPOC according to the guidelines. First, the Interpol department will move into the same location as the other channels. Then, a common operational centre will be created, which will be the single point of entrance. After that, a new technical infrastructure, including case-management system and archiving system, needs to be developed.

Greece applied for EUR 1 000 000 funding from the ISF (Internal Security Fund). This transformation is expected to be finalised by mid-2016.

Regarding the possible future development of the concept, we note here that there are some plans in Finland for developing the current front office into a Situation Centre with analysts and intelligence.

Our assessment below on the application of the concept of SPOC in the Member States looks at it from the following perspective:

- Implementation of the EIXM Communication criteria;
- Implementation of the SPOC Guidelines criteria;
- Different models of the functioning of the SPOC; as well as
- Added value, difficulties and limitations.

a) Implementation of the EIXM Communication criteria

The specific **criteria** for SPOCs in the **EIXM Communication** are: covering all main channels, available 24/7, and bringing together all law enforcement authorities, with access to national databases.

Covering all main channels seems to be generally accepted as a prime condition for a SPOC. We observe based on our fieldwork and phone interviews that **normally all three main channels** (i.e. Europol, Interpol, SIRENE) **are covered** by Member States' SPOCs. However, as detailed in section 4.2.2.3, SIENA is in many cases not used to a significant extent. Furthermore, in most countries not all SPOC staff members can use all channels, especially in those countries where there are different teams designated to work in the front and in the back office. SPOCs are **available 24/7**, except that most Member States do not monitor SIENA outside office hours. As also highlighted in the section on the choice of channel, this is actually a vicious circle as interviewees regarded it as in "the nature of SIENA" not to be fed at night and, in the absence of an actual legal obligation to do so, they do not work with it then either as they do not see any communication coming in on it. As also mentioned in section 4.2.2.3, this is also related to the fact that SIENA is in many Member States only available to the ENUs, which usually do not operate on a 24/7 basis.

Regarding the criterion of implementing a **multi-agency model**[128], we note that less than half of the Member States seem to have such a system in place.[129] The most typical law enforcement authority other than the police (or gendarmerie) to be present in a SPOC is customs. Some Member States also have finance or coast guard staff working in the SPOC.

In terms of the criterion of SPOCs' access to **national databases** no issue was reported during our interviews.

[128] I.e. in which different law enforcement authorities other than the police are present.
[129] Source: SPOC Guidelines Addendum.

Most Member State SPOCs do not have a **manual** for the choice of channel. This is particularly interesting in view of our observation reported under section 4.3.1.1, i.e. that SPOC officers do not in general receive hands-on onboarding training.

b) Implementation of the SPOC Guidelines' criteria

The June 2014 **SPOC Guidelines** set criteria in addition to those defined by the EIXM Communication. Our assessment of the current implementation of these is presented in the Table below.

Table 4: Application of the SPOC Guidelines' criteria in the Member States

SPOC Guidelines' criteria	Our assessment[130]
The SPOC has **one phone number and one e-mail address** for all international police cooperation requests sent at central level.	SPOCs in most Member States have more than one e-mail address.
Ideally, the SPOC houses its different sections in the **same building**.	There is a mixed picture in this respect for Member State SPOCs. We also note that some sections of the SPOC, even though they are in the same building, can sometimes be housed on separate floors.
Its staff - includes interpretation or translation capacities; - is trained and equipped/mandated to deal with all kinds of tasks.	Translation capacities do not seem to be present in all structures. As mentioned in section 4.3.1.1, staff onboarding training is limited.
Every investigating police officer knows the basic services provided by the SPOC.	Interviewees and our web-based survey results[131] reveal ample space for improvement in this respect.
A **request** is sent through **one channel only**[132].	Due to the diversity of national preferences for the choice of channel, duplication still remains.
The SPOC has access to a **case management system** that evaluates, classifies and disseminates the information originating from all cooperation channels and national authorities.	Not all Member States have a case management system for the SPOC.
Staff are able to communicate orally and to have good written skills in the most relevant foreign languages for this country. Operators all speak **English**.	There is room for improvement in most Member States.

[130] Colour coding: red stands for "ample space for improvement", orange stands for "space for improvement".

[131] In our web-based survey, respondents were first asked whether a SPOC exists in their Member State. It is striking that more than one quarter of them (27.7%) indicated "I do not know", which could either relate to a lack of knowledge about the concept of a SPOC or to a lack of a general definition of the concept of SPOC.
When asked about the different features of their SPOC, responses were rather similar between SPOC officers and policy makers. For all features (except the use of the UMF II data model), the majority of respondents indicated that the feature exists in their Member State. However, the proportion was lower among the SPOC officers.

[132] If a request is, in exceptional cases, sent through different channels at the same time, this is clearly indicated on the request.

As the table above shows, for the most part the criteria of the SPOC Guidelines are not yet implemented in practice.

c) Different models for the functioning of the SPOC

Overall, almost all interviewees considered the SPOC concept as **highly useful** and conducive to facilitating information exchange. Some even consider it the main element establishing information exchange among Member States. In addition, many highlighted that, besides providing a contact point for international contacts, having a convergent point for international cooperation in this form is also useful for coordination within the country.

However, apart from the definition of the SPOC (detailed above), the understanding and implementation of its *modus operandi* also varies across Member States. We note in particular diversity over:

- Functioning as a coordinating office (civilian staff)[133] versus a more prominent overview role (where staff has substantial subject matter expertise)[134].
- Designated separate front office and back office teams versus a mixed model where staff can have an overview of both roles.
- Different level of empowerment of field officers[135]. This can result in, for example:
  - some SPOCs using the channel that their requesting investigators indicate they prefer while others make this choice independently; or that
  - field officers in some Member State have direct access to SIENA.[136]
- The extent to which law enforcement agencies other than the police are involved.

We observe that these different models entail different levels of efficiency in facilitating information exchange, and are also closely linked to the national traditions and the national landscape of law enforcement institutions. Nevertheless, based on our interviews and expert panel, we observe that overall, establishment of a SPOC seems to depend mostly on **political will**. In this respect the adoption of the Guidelines seem to have inspired reflection in some Member States on how to adapt the organisation of their SPOCs[137], but this process still is voluntary and hence remains limited in scope.

d) Added value, difficulties and limitations

In general, our interviewees and expert panel participants perceived that there is substantial **added value** in having a SPOC. It is felt that the SPOC plays an important role to avoid duplication. Furthermore, the SPOC is also believed to be in place to ensure quality of messaging, and to have an overview function (which is the reason why it is seen as important by many that the SPOC is involved in all exchanges).

---

[133] Some interviewees believed that civilian staff need more explanations from the requesting Member State than actual police staff. However the Nordic countries seem to have positive experiences with having civilians working in the SPOC.
[134] This choice also depends on e.g. the language knowledge of field officers.
[135] NB in urgent cases, e.g. in Finland and in Hungary, field officers can inform the SPOC only after a request was sent out. In these cases an ex post notification is made to the SPOC. We note that in this solution, not only is the workload less for the SPOC, but it also has less relevance, which also entails some risks. These can however be balanced and managed according to our interviewees.
[136] This in some Member States entails the possibility of actually sending requests autonomously or sending a draft version of the request in SIENA to the SPOC which then sends out the finalised message.
[137] Or similar international police cooperation structures as applicable.

Expert panel participants also highlighted that SPOCs can mitigate the controversy on the choice of channels – *provided* all channels are available to a SPOC and the SPOC is able and ready to use all channels appropriately (including e.g. information sharing with Europol).

Furthermore, some panel participants believed that as a general rule, police officers need the SPOC as a connecting piece between them and another legal system, where they do not know the legal standards and the language. Some interviewees stated that for them it is easier to communicate with a Member State that has a SPOC, because it is more efficient.

Those interviewees, who expressed a view of the subject, believed that the SPOC concept was a good way of maintaining quality of data, as it allows for officers to be better trained in data protection.

In Member States where the SPOC concept is not yet implemented, interviewees reported that there were cases where, without being aware of it, different international police cooperation units were working on the same case, because they received the same request through different channels.

Case example: Challenges in the absence of a SPOC

Before Bulgaria and Romania's Schengen accession, the Interpol units handled requests from these countries. In Member States without SPOC and no common case management system, the SIRENE Bureau seems to have to contact the Interpol unit about cases involving these countries to find out about any relevant old cases.

Furthermore, in the absence of a SPOC, there are in some cases no direct connections between e.g. the Europol and the SIRENE units, with officers not being exactly sure what their colleagues in the other unit actually do.

As mentioned above, not all Member States have a SPOC fulfilling the criteria of the EIXM Communication and the SPOC Guidelines. Our interviewee specifically mentioned some **difficulties** with establishing comprehensive SPOCs. Lack of resources can be a difficulty, however we note that once in place, SPOCs can also, via rationalisation of resources, entail savings.

Rigid national organisational structures and resistance to change can pose another difficulty in developing a SPOC. In fact, even once it is there, **as efficient as the SPOC may be, it cannot in itself overcome less efficient ways of working further afield in the national administrations**.

For example, while SPOCs might work with an email-based case management system to sort out and allocate work to its staff, their national "clients" in the field often still use paper files or fax. Inserting and formatting these messages into the SPOC's system takes resources and these issues have an effect on the response time for requests. Hence we observe that national workflow challenges are exported to the EU level, with some Member States being known among the rest of the Member States as very frequently replying late to requests.

Furthermore, there is often a division or even competition of competence between national entities, which is not overcome by the installation of a SPOC.

As an additional issue, we highlight the question of the **language of communication** among SPOCs. The most common language is English. However, it is not the only language used. In particular, many interviewees highlighted that they use their own language with specific countries that can understand

it.[138] Although substantial misunderstandings due to language use were not reported, most of our interviews acknowledged that there is still space for improving SPOC staffs' language skills.

Case example: Language of communications

We note here the example of Hungary where simplicity in the use of foreign languages is promoted for SPOC staff. They furthermore have at their disposal a simplified English vocabulary the aim of which is to allow the staff to communicate efficiently using the most simple but most descriptive words in their communications.

The issue of languages is especially crucial in the front office. Some SPOCs only run reduced language capacities outside of normal working hours.

While, in general, there is wide appreciation among stakeholders for having a SPOC, a few also mentioned what they see as the **disadvantages** of this concept.

While acknowledging that SPOCs bring consistency in the way requests are treated, some nevertheless believed that incoming requests are interpreted according to the national law of the requested state. This can relate to national rules regarding deadlines for response, the national approach to only limiting the reply strictly to the information requested, as well as specific national data protection rules.

As another limitation, some interviewees mentioned the fact that due to the alertness needed and the shifts they work in, staff switching between shifts in both front and back office[139] can be overworked.

In those Member States where the SPOC has a strict coordinating role, some interviewees saw it as a limitation that this obligatory involvement of the SPOC actually prolongs the distance (and hence the time elapsed) between information source and end use.

4.2.1.2 The role of PCCCs, cooperation between SPOCs and EUROSUR NCCs

Our interviewees and expert panel participants agreed that there can be a number of exceptions to the SPOC concept. FIUs, terrorism units and PCCCs (Police and Customs Cooperation Centres) were also mentioned by our interviewees and expert panel participants as requiring very specific expertise, and are specifically confidential or fall under very specific legislation.

PCCCs were set up at internal borders on the basis of the Schengen Convention in order to address the "security deficits" in border regions. They are located at strategic positions and bring together, on one site, all the security authorities of all participating States.

A significant proportion of police information exchanges are believed to take place via PCCCs[140], which in many cases are believed to occur without the SPOC being made aware of them. We note that this could, to a certain extent, hamper a good information exchange and also limits the statistics that could be gathered on the information exchange. Moreover, it prevents the SPOC from transmitting such information, where appropriate, to a central analysis capacity.

The EIXM Communication pointed out that the generally high number of exchanges mostly do not concern the most serious and organised crime, but it is nevertheless a challenge to ensure that information on relevant cases is passed up to national (SPOC) level and, where appropriate, to Europol. Our study has not received any indication of this not being the case. Indeed, according to our

[138] E.g. Germany uses German when communicating with Austria, the Netherlands, Denmark and some others.

[139] Which in itself is deemed beneficial for their ability to have an overview and hence make a more informed choice of channel.

[140] Their number was 38 at end 2011 according to the EIXM Communication.

interviewees, exchanges between PCCCs without the involvement of their SPOCs are expected to be restricted to cases with regional relevance, and in these domains an involvement of the SPOC is not deemed desirable.

Nevertheless, it was pointed out during our interviews that while PCCCs are generally functioning well, they lack a commonly agreed legal framework. In fact some examples (e.g. regarding follow up after a SIS alert) were reported by several of our interviewees in which a chain-communication was conducted between PCCCs, avoiding the involvement of SPOCs along the way. We note that in principle the SPOC receives an *ex post* notification of these exchanges.

The EIXM Communication further notes that annual conferences at EU level enable sharing of experiences and common approaches. We note here the example of Hungary where PCCC leaders meet annually with the SPOC.

The **EUROSUR** Regulation[141] establishes a common framework for the exchange of information and cooperation between Member States and Frontex in order to improve the situational awareness[142] and reaction capability at the external borders. In order to coordinate national border-control activities and to collate and exchange information between their various border-control and law-enforcement bodies, Member States established National Coordination Centres (NCCs).

Member States have operated NCCs 24/7 as of 2 December 2013 at eastern and southern external borders, and as of 1 December 2014 NCCs at all land and sea external borders.

The cooperation and information exchange between the national coordination centres and Frontex occurs via 'situational pictures', which are established at national and European level as well as for the pre-frontier area.

With the implementation period not being passed for all Member States during the data collection period for this study, no particular information was received about cooperation between SPOCs and EUROSUR NCCs.

4.2.1.3 Conclusions

The vast majority of Member States have an international police cooperation structure that at least partly complies with the Single Point of Contact (SPOC) criteria set by the EIXM Communication and the subsequent SPOC Guidelines.

Those not having a SPOC face difficulties with optimising their workflow which is constantly increasing as cross-border information exchange expands.

The concept of the SPOC is considered as highly useful and as clearly facilitating information exchange. However, application of the SPOC concept varies across Member States and there is no common understanding of what constitutes a SPOC and how to assess whether different features exist.

The adoption of the Guidelines seem to have inspired reflection on how to adapt the organisation of the SPOCs organisation, but this process still is voluntary and hence remains limited in scope.

[141] The Regulation is applicable as of 1 October 2013.

[142] "Situational awareness" is a measure of a Member State's ability to detect cross-border movements and to take rational control measures based on evidence.

4.2.1.4 Recommendations

- The SPOC Guidelines need to be transposed into the national context by the individual Member States. The application of the Guidelines' in the Member States should be evaluated by the Commission in two years from now.
- Consideration should be given to establishing a network consisting of SPOC staff and/or heads of SPOCs with a view to exchanging good practices and lessons learned, as well as identifying issues related to the application of the SPOC Guidelines and in particular to the choice of channel.
- Member States are invited to facilitate, with the support of Commission funding, the use of all channels equally by establishing electronic case management systems for their SPOC. More specifically, without prejudice to relevant data protection standards, a national interface could be created that makes it easy to use all different channels.
- Integrated solutions should be adopted where officers in the field do not have to choose the information channel, but it is built into routines and national systems.
- SIRENE manual and good practices should, where appropriate, be taken into account when shaping the setup of SPOCs.
- Member States should also ensure that the workflow is clear between the SPOC and the PCCCs.
- As it is not sufficient only to improve the SPOCs, in cases where the national workflow outside the SPOC lacks efficiency, attention should be also paid to optimising workflow from field officers to the SPOC.
- In order to ensure timely implementation, a peer evaluation mechanism should be devised for Member States' SPOCs.

4.2.2 The channels used for information exchange

As explained under section 3.4, there are three main EU and international channels used for cross-border information exchange, i.e.: (1) SIRENE, (2) the Europol channel, and (3) the Interpol channel. Bilateral or regional channels are used in addition to these channels, such as the regional PCCCs. It was highlighted in the EIXM Communication that the choice of information channel is only partly regulated by EU legislation.

In the EIXM Communication, the Commission found that there are currently different approaches on the choice of channels and invited Member States:

- For exchanges where the channel is not legally defined, to use the Europol channel using the SIENA tool as the default channel, unless there are specific reasons to use another;
- To develop national instructions for choice of channel;
- In particular, after SIS II went live and once SISNET was closed, to use the Europol channel and SIENA tool for police cooperation exchanges using SISNET.

In addition, the Council was invited to:

- Amend EU-level guidance to reflect the choice of channel guidelines suggested in the EIXM Communication.

The Commission indicated that it would:

- Participate in work to assess the feasibility of an Information Exchange Platform.

The following sub-sections outline the developments in this area since the adoption of the EIXM and the remaining gaps under the following headings:

- Instructions and Guidelines;
- National approaches and difficulties encountered;
- Practices relating to the use of SIENA and difficulties encountered in this regard; and
- Feasibility of standardisation of the use of the different channels and SIENA.

4.2.2.1 Instructions and guidelines

EU-level guidelines on the choice of channel have been developed on several occasions. In the 2008 *Manual of Good Practices concerning the International Police Cooperation Units at National Level*, four main criteria[143] were mentioned: geographical approach, thematic approach, technical approach, and urgency.

The SPOC Guidelines adopted by the Council in June 2014 also include specific criteria on the choice of channel. They stipulate general rules on international exchanges, including that requests should normally only be sent via one channel, that the channel should normally not be changed during on-going operations.

[143] These are also reflected in the *Guidelines on the implementation of 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*, 9512/1/10 REV 1 (http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209512%202010%20REV%201).

The SPOC Guidelines list the possible channels and give suggestions of how to use these (see the box below).

Criteria on the choice of channel suggested in the 2014 SPOC Guidelines[144]

Europol

- *EU reach and its mandate (terrorism, serious and organised crime, two or more MS concerned),*
- *Contributions to AWF, EMPACT projects*[145]*, analysis, JITs (Joint Investigation Teams),*
- *Exchange of classified information (up to EU RESTRICTED),*
- *Exchange under Swedish Framework Decision (SIENA form/UMF),*
- *Urgency.*

Interpol

- *Exchange of information with EU Member States and third countries,*
- *Alerts (wanted/missing persons, arrest warrants, extraditions),*
- *Verification of person's identity/documents,*
- *24/7 availability and urgency.*

SIRENE

- *SIS alerts,*
- *Cross-border surveillance,*
- *24/7 availability and urgency,.*

Bilateral/regional channels

- *Exchange of classified information (depends on terms of bilateral agreements),*
- *Urgency, trust.*

PCCC

- *Local reach and exchange of information about crimes committed in the border area; Naples II*[146]*/AFIS*[147]*/CIS*[148]*/FIDE*[149]*/FIU*[150]*,*
- *Specific information exchange/ legal assistance.*

Instructions or manuals on the choice of channel seem to exist in a number of Member States but not in all. Some Member States have clear guidelines, e.g. on one page to ensure that officers can get a quick overview. However, where they exist, they are usually not binding. Indeed, in some Member States, there is a lack of political will to define stricter manuals, as there is a strong tradition of leaving the choice up to the law enforcement officer.[151] Yet, in a few Member States, general instructions are

[144] *Draft SPOC Guidelines for cross-border law enforcement information exchange,* Council Document 10492/14.
[145] European Multidisciplinary Platform against Criminal Threats; See: https://www.europol.europa.eu/content/eu-policy-cycle-empact.
[146] Council Act 98/C 24/01 of 18 December 1997 drawing up the Convention on mutual assistance and cooperation between customs administrations (Naples II Convention).
[147] Automated Fingerprint Identification Systems.
[148] Customs Information System, set up based on Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31997R0515).http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31997R0515).
[149] Customs file identification database.
[150] Financial Intelligence Unit.
[151] We noted here that there is a desire for stricter rules among certain stakeholders, which is discussed in section 4.2.2.4.

even contained in a legal act, e.g. a decree transposing the SFD. Based on the conflicting views found in our web-based survey or interviews, not all officers know about the existing instructions.

Where they do exist, instructions are generally perceived as helpful. Our web-based survey inquired how useful the instructions are for field officers and SPOC officers. The majority of respondents to the WBS in both function groups agreed fully or somewhat with the following three statements:

- They are sufficiently detailed, i.e. they provide clear explanations for my cases;
- They are helpful, i.e. they have an added value for my work; and
- The officers I know actually use the procedures described by the instructions/manual.

A small share of persons from both function groups indicated that they disagreed with these statements. The first statement regarding the level of detail of the instructions received the highest level of disagreement from both groups: 20% of field officers and 13% of SPOC staff indicated that they do not consider the instructions to be sufficiently detailed. About 10% of both groups indicated that they do not consider the instructions to be helpful and suggested that the procedures described in the instructions are only used to a limited extent.

Example: Belgium – Efforts to increase awareness with regard to the choice of channel

A lot of effort has been put by the Belgian SPOC into raising awareness in relation to international information exchange. A specific "Choice of channels" guideline has been developed and presented to all police forces of Belgium. It is also published on their Intranet. Updated Guidelines are distributed, with clear procedures and business rules on international information exchange and there have been specific course modules. This has resulted in an increasing awareness and better use of information exchange tools and channels. Although there is still work to do, these activities have contributed to significant improvements in the past few years.

4.2.2.2 National approaches and difficulties encountered

As further outlined in section 4.2.1, the SPOCs play an important role in ensuring appropriate choices of channels as well as avoiding duplication. Only in a few Member States can the channel be suggested or chosen by local units. If local units are involved, they are normally supported by the SPOC.

The **approaches towards choosing which channel to use vary across Member States and sometimes even within Member States**. Based on the research activities carried out for this study, many officers still decide on a case-by-case basis.[152] When discussing the considerations that apply when an officer is deciding which channel is appropriate, our interviewees mentioned various different factors. In some situations, EU or national instructions are taken into account, while personal considerations prevail in other situations. The following factors play a role to a greater or lesser extent:

- **Guidelines/instructions developed at EU level or national level**. This point was discussed in the previous sub-section.
- **The incoming channel**. In almost all cases, SPOC officers reply via the channel that was used by the requesting Member State unless there is a legitimate reason not to (e.g. it is only later discovered that third countries are involved). There are very few instances where SPOC officers reply via a different channel for other reasons, such as their own preferences.
- **Urgency.** Officers take into account whether a channel is likely to bring fast results, including considering the time of the day. This is taken into account in particular for the use of SIENA,

[152] This was also noted in 2008 by the *Manual of Good Practices concerning the International Police Cooperation Units at National Level* (Council document 7968/08) that pointed to a lack of guidance in this regard.

which is currently not available on a 24/7 basis in all Member States. In addition, some interviewees note that they have a perception of whether a particular channel is faster than the others, e.g. because less work is involved in requesting information or because the other Member States usually react faster.

- **The purpose**. If information is needed as evidence, official requests are needed; at early stages of the investigations, a call might be suitable just to get an idea of whether a Member States might have relevant information.
- **Officers' personal preferences or habits.** Some officers have preferences, e.g. because a certain channel is easier to use, they are more familiar with it, or it brings better (i.e. faster or more comprehensive) results in their experience.
- **Counterpart preferences**. Some Member States are more flexible with regard to the choice of channels, e.g. because the structure of their SPOC allows all officers to access all channels. Therefore, some Member States instruct their officer to use the channel that is preferred by the requesting counterpart.
- **Need for security**. Consideration is also given to whether or not the information exchanged is classified or particularly sensitive. In such cases, some law enforcement officers prefer exchanging information via Liaison Officers, for example.
- **Size of the companies or criminal networks involved**. For example, one officer dealing with financial crimes indicated that a request relating to a major fraud would be dealt with most effectively via the Europol channel (as compared to the Interpol channel). This is because large companies or networks are usually known to Europol.

Thus, the individual channels are used in different situations. We note that the choice of channel is open (i.e. not defined by law) for Prüm follow-up requests, which are discussed separately in section 4.1.2.2, as well as SFD requests in general.

In general terms, the biggest overlaps are between Europol and Interpol channels.[153] The choice depends on the persons involved, the particularities of the case, and the set-up of the SPOC. The **Europol channel** is often still associated with Europol's mandate, although the use of the channel is no longer limited to this. The use of SIENA varies across Member States. This is discussed in sub-section 4.2.2.2. Although the **Interpol channel** is generally mainly meant for exchanges involving third countries, it is in many cases also used for pure EU cases, as also demonstrated in section 4.1.2.2 on Prüm follow-up requests. The Interpol channel is popular among officers, mainly because of its free text format, guaranteed 24/7 availability and the tradition of using this channel. Based on the interviews and our web-based survey, several Member States clearly prefer using the Interpol channel over other channels. This is in some cases also reflected in existing national instructions. Some interviewees estimate that Interpol is the channel that is used most often in the context of police cooperation.

No major difficulties have been reported with the use of **SIRENE**. For most interviewees, it seems to be clear when to use the SIRENE channel. Many indicated it is used whenever a case has a Schengen ID or concerns a Schengen alert. Yet, it is not clear to all interviews that SIRENE is not meant to be used for exchanging information that is not related to supplementary SIS data, in particular for requests under Article 39 CISA (see also section 4.1.1.4).

There is no agreed solution for **information previously sent via SISNET** for police cooperation purposes. A few interviewees from ministries and law enforcement services regretted that it has not

[153] *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD 2010 (http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/icmpd_study_lea_infoex.pdf).

been clearly determined that SIENA could be used for this purpose. Based on our fieldwork, SIRENE and the dedicated SIS II network is in fact still used for such exchanges in many Member States, although it is not supposed to be used for this purpose any longer. In many Member States, Interpol is favoured for such exchanges.

The **PCCCs** are appreciated for complex regional cases in particular, as investigators from different Member States can work together and have direct access to several databases. The division of tasks between the PCCCs and the SPOCs is relatively clear. However, some interviewees and participants in the expert panel pointed out difficulties with so-called "chain requests". In a hypothetical example, a Spanish officer could be interested in information from Germany. Instead of contacting the SPOC, he sends a request to the PCCC for France-Spain, which could then forward the request to another PCCC for France-Germany.

In addition to these formal channels, **informal communication** plays an important role. The extent to which informal communication channels are used is impossible to estimate. Several interviewees mentioned that there are situations in which informal communication would be favoured, at least initially. For example, if it is important to know very quickly whether or not relevant information exists, a call may help. An official request would then be sent later, as this is needed in order to use information in a judicial procedure. Informal communication is also used in parallel to formal requests e.g. to make SPOC officers aware of a very urgent request. Thus, in most cases, informal exchanges are related to or followed up by formal requests.[154]

There are differences across Member States in openness to informal exchanges. Some interviewees reported that it is difficult if such direct exchanges are not known to the SPOC. In addition, an officer might have to spend more time on one case if there are both formal and informal contacts. However, other interviewees and respondents to our web-based survey stressed that informal communication can help cross-border information exchange, because in some cases it can speed up the procedures. Moreover, informal communication fosters trust in other Member States and information exchange in general. This was highlighted in particular by officers who have participated in a staff exchange.

Requests are sometimes sent via two channels. According to the interviews carried out for this study, this causes problems only in Member States where the different channels are not connected within one case management system. In Member States where this exists, duplication can normally be detected.

4.2.2.3 Practices in the use of SIENA and difficulties encountered

Since the EIXM Communication, **some steps have been taken at the EU level in the direction of developing SIENA as the primary tool for cross-border information exchange**.

There have been some initiatives to improve the functioning of SIENA. A roadmap for attaining this objective has been prepared by the Heads of Europol National units (HENU).[155] Some of the policymakers consulted regretted that this roadmap currently does not have sufficient political weight to be effective. Europol is planning to support Member States in overcoming constraints in using SIENA,

[154] This is also highlighted by the *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD 2010 (http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/icmpd_study_lea_infoex.pdf).

[155] HENU Workshop on SIENA Implementation - Roadmap on SIENA implementation, 2014, Council doc 10303/14 (available at: http://www.parlament.gv.at/PAKT/EU/XXV/EU/02/71/EU_27196/imfname_10470533.pdf)

including e.g. support in connecting SIENA to the national case management system.[156] To this end, Europol has initiated a survey about Member State's difficulties with SIENA and is planning to work on the problematic areas[157].

In the recently adopted SPOC Guidelines, the Presidency "recommends to thoroughly examine the use of SIENA III as the prime tool for exchanging operational and strategic intra-EU crime related information and intelligence, both with regard to the Europol mandate and to bilateral information exchange between Member States."[158]

In spite of these steps, the findings of this study show that there is currently no consistent understanding of the use of SIENA and there are big differences relating to its use in the Member States. In addition, there are still some practical factors hindering the use of SIENA (which have been partially taken into account by the initiatives mentioned above).

The extent to which SIENA is currently used in the Member States varies. In some Member States, access to SIENA is limited to the ENU. In a few Member States, only the Europol Liaison Officer (ELO) can access SIENA, because there are difficulties relating to accreditation. In others the SIENA *application* is only available to officers in the ENUs, whereas some additional departments, in particular in the SPOC, make use of the *web service***.**

A number of Member States are working on making SIENA available to the wider circle of end-users. For example, it was reported by an interviewee (manager in a law enforcement authority) that in Germany about 50% of investigators can fill in forms directly. According to another interviewee, Finland has approximately 330 trained SIENA users, of whom approximately 260 are active users. Other sources support the evidence for increased use of SIENA by different authorities in the Member States: according to Europol, 452 competent authorities representing 4 150 users were configured in SIENA by the end of 2013. These come primarily from the 28 EU Member States, but include 42 authorities in third states. The number of new cases initiated in 2013 was 18 310 new cases, of which 85% were initiated by Member States. The number of new cases initiated has been increasing since 2005 (there was a 15% increase between 2012 and 2013.)[159]

In spite of these developments, the findings of this study indicate that **the Europol channel using SIENA is so far promoted as the main channel only in few Member States** (including e.g. BE, BG, CY). For example, in Belgium SIENA is the priority channel for information exchanges within the European Union. Belgium has extended SIENA to the central crime directorates, one PCCC (Heerlen) and also to the provincial level. However, SIENA is in many Member States still considered as being reserved for ENU and specific Europol cases, not for SFD and Prüm.

Some Member States have been facing **difficulties with the use of SIENA in general and also with the efforts in making SIENA available to more stakeholders.** Indeed, this was raised by many interviewees and some respondents to the web-based survey. This is confirmed by the survey carried out by Europol, according to which 39 % (11) of the Member States identified constraints at national level to working

---

[156] Powerpoint on "SIENA – Member States' constraints" of 2013 provided by Europol; HENU Workshop on SIENA Implementation - Roadmap on SIENA implementation, 2014, Council doc 10303/14 (available at: http://www.parlament.gv.at/PAKT/EU/XXV/EU/02/71/EU_27196/imfname_10470533.pdf).

[157] *SIENA – Capture Member States' constraints*, Europol 2013, CM 3878/13. Europol is planning to implement some changes in the future in order to overcome the constraints, including a multilingual interface, structured data and connection to the national case management systems (Powerpoint on "SIENA – Member States' constraints" of 2013 provided by Europol).

[158] *Draft SPOC Guidelines for cross-border law enforcement information exchange, EL Presidency 2014,* http://data.consilium.europa.eu/doc/document/ST-6721-2014-REV-3/en/pdf.

[159] *Europol Review 2013 (* https://www.europol.europa.eu/content/europol-review-2013).

with SIENA.[160] The following paragraphs give an overview of the most relevant difficulties/constraints that were highlighted to us in the research activities carried out for this study.

From a practical point of view, the fact that SIENA is **not monitored on a 24/7 basis in the Member States** is one of the main factors standing in the way of a broader use of SIENA. Only a few Member States have 24/7 presence on SIENA. SIENA is used mainly by the ENUs in many Member States. Many of them are, however, not operational on a 24/7 basis. Only a few Member States also offer access to SIENA for their 24/7 departments. Several interviewees noted that this is one of the most relevant factors for SIENA not being used more often. For example, one interviewee explained that, while they have access to SIENA in the 24/7 department, she would not use SIENA out of business hours upon her own initiative, because there is a risk that there is nobody to open the mailbox in the other country. If she received a request via SIENA e.g. on a Friday afternoon, she would at least call the requesting Member State first to ensure that a response would be opened. This can be a vicious circle: SIENA is not used because it is not available in Member States on a 24/7 basis. Since it is not used, there is no reason for Member States to make an effort to set up 24/7 availability.

Some officers raised another restriction, namely that it is cumbersome to work with SIENA, because it is **not integrated into the national case management system**. Thus, there is too much manual work involved.[161] For example, there is a view that it is easier to work with Interpol than with SIENA, because Interpol uses XML format, which can be read in an email programme. In contrast, using SIENA is more difficult according to several interviewees, because messages cannot be read directly in email format. Officers in specialised departments do not have access to SIENA. They prepare the response and forward it to colleagues in the Europol units, who then transfer it to the system.[162] SIENA messages thus first need to be downloaded and converted before it is possible to transfer them to the case management system. For complex cases, requests need to be translated. Thus, the relevant information needs to be copied into an email, which can then be forwarded to the translation department. When the translated text is back, it can be forwarded to the relevant specialised department if necessary. To send a reply, the content again needs to be transferred to the form. Such intermediate steps are not necessary for Interpol messages, which are transmitted directly.

It is possible to connect SIENA to national case management systems. This facilitates reception of messages in the national systems.[163] Based on the views on the restrictions of SIENA outlined above, not all practitioners interviewed at SPOC level know this yet. Often the restrictions were associated specifically with SIENA as a tool, not with the way this tool is used in the respective Member States. The first Member State that made use of this interconnection between SIENA and the case management system was Germany.

A third restriction relates to the use of the forms within SIENA. Some argued that exchange via SIENA requires more work than the Interpol channel because the **form contains information that is not necessary or causes confusion**. For example, the handling codes are not necessary in the view of some interviewees, because in principle information is rarely restricted. When it is, it would be easier to add

[160] Powerpoint presentation on "SIENA – Member States' constraints" of 2013 provided by Europol.
[161] See also *Study on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records System,* (2012), indicating that "currently most of SIENA related activities/processes are manually driven".
[162] Some specialised departments that are related to organised crime do have access to the SIENA application or web service.
[163] Cf. *Europol Review 2012 (*https://www.europol.europa.eu/sites/default/files/publications/europolreview2012_0.pdf*),* p. 15.

text instead of ticking boxes with codes. The handling codes do not seem to be clear to everybody and are sometimes used incorrectly, making it necessary to send follow-up messages.

Furthermore, some interviewees noted that **the quality of information** received via Interpol is generally better than that in SIENA. In SIENA, data is often missing according to the experience of some interviewees, making it necessary to send another request. This was explained by the fact that there are too many fields to fill in, which takes time, and that the purpose of all fields is not well-understood by all officers, leading to omissions.

Another practical problem raised by some of the interviewees is that due to the **high security requirements**, case officers are often logged off automatically and need to log on again, which takes time.

Based on information provided by Europol, six Member States indicated that that the **current classification of SIENA as "EU restricted"** causes difficulties.[164] This was confirmed and explained during the interviews carried out for this study. The classification has been causing delays in the implementation because complex measures are necessary before access to SIENA can be granted. In addition, there are specific requirements for the use of SIENA, which can complicate the integration of SIENA into national workflow systems.

It is difficult in the Member States to find solutions for granting **direct access to SIENA to field officers and at the same time ensure that the SPOC has an overview** of all exchanges. In addition, a wider use of SIENA in the field requires additional training and a change of mind-set, as the extent to which field officers are directly involved would increase, as specifically highlighted by some policy makers interviewed for this study.[165]

A final practical difficulty that surfaced is the fact that **most stakeholders think that English** must be used for sending SIENA messages. Indeed, the use of English is considered a disincentive by many interviewees and some participants in the expert panel. This seems to be a misunderstanding: Any language can be used in SIENA. It is only for sharing data with Europol via SIENA that English is recommended. Practitioners also noted that the need for translation is lower when using the Interpol channel, because messages can be forwarded in any language that the counterpart can understand.

In addition to these practical difficulties, there are **difficulties relating to personal attitudes**. Some officers see SIENA as a threat to their established ways of working. Habit is another reason for the limited use of SIENA.

Moreover, **awareness of SIENA and its offers is limited.** This was also highlighted during the expert panel. We received indications that there is a lack of training on SIENA in some Member States. Some feel that the SPOC could be more active in this regard if the intent is to increase the use of SIENA. For example, one interviewee explained that many officers in the 24/7 department are currently sceptical, which is why it is relevant that the benefits of SIENA be better explained. **Thus, some of the practical difficulties reported on above may be based on a lack of awareness.**[166]

---

[164] Powerpoint presentation on "SIENA – Member States' constraints" of 2013 provided by Europol.

[165] This point was also made by Kattge, L. (2013). *The Europol channel in the system of multilateral cooperation in the EU,* Master's dissertation, p. 84-85.

[166] This in line with the findings of Kattge, L. (2013). *The Europol channel in the system of multilateral cooperation in the EU,* Master's dissertation.

4.2.2.4 Feasibility of standardisation of the use of the different channels and SIENA

There are mixed perceptions as to whether standardisation is desirable. The interviewees and participants in the expert panel had different views on the extent to which the current situation with regard to the choice of channel poses challenges. Some stakeholders argued that the current situation is too chaotic. For example, there are cases where a response is not sent via the same channel as the request or where requests are sent via different channels. As highlighted above, Member States use the channels for varying purposes and to a varying extent.

Other stakeholders argued that the current situation does not pose any challenges because the choice of channel is a domestic management issue. No strict rules are needed, but rather guidance. These participants noted that the difficulties associated with the open choice of channel are mainly based on domestic workflow problems.

Experts are split on whether the choice of channels becomes obsolete if a SPOC is in place. Some interviewees and participants in the expert panel indicated that the choice of channel is no longer an issue as soon as Member States have a SPOC, where all channels can be accessed centrally.[167] During the expert panel, it was noted by other participants that the choice of channel will remain relevant even once SPOCs are fully implemented. In particular, it was explained that the issues would only become obsolete if all channels were equally accessible via one system and available on a 24/7 basis within all SPOCs. In addition, it was pointed out that the choice of channel does make a difference for Member States' ability to share information with Europol.

Perceptions of the feasibility and desirability of making the Europol channel using SIENA the default channel for EU communication are somewhat mixed. While a large number of interviewees argued that it would be desirable to further promote the use of SIENA for SFD, Prüm and Europol requests, others were critical. The criticism related to the challenges highlighted in the previous sub-section, while the arguments that working with SIENA is more cumbersome and that it is not monitored on a 24/7 basis were put forward most frequently. The Council, in its Conclusions on the EIXM, invited Member States to consider using SIENA for the exchange of information within the context of police cooperation, but underlined the possibilities of using other channels. This implies that not all Member States consider it useful to promote SIENA as the main channel in the EU.

In addition, some stakeholders argued from a more general perspective that it would not be desirable to impose *any* channel as the choice should remain up to the desk officer to allow for sufficient flexibility. It would not be a good idea to use it as a single channel, because there must be an alternative in case there is a technical issue.

Those who were positive about its use argued that **SIENA provides the opportunity to exchange information by using high security and data protection standards without much effort**. Anybody who can use Outlook would be able to use SIENA. From the operational perspective, SIENA is useful for complex[168] cases as it works very well as a case management system: it is possible to see how many recipients of a request have already responded; it is possible to give a partial answer in order to provide a quick reply; it contains reminders; it can also be used internally between the different national services.

[167] This is further discussed in section 4.2.1 on the *The Single Points of Contact (SPOCs)*.

[168] Example: fingerprints of a prostitute who is suspected of also smuggling drugs – it falls under the competence of many different units of the police.

The EDPS noted that harmonisation is generally welcomed. However, at the same time, the EDPS underlined that the possible consequences with regard to data protection should be considered.[169]

Another more strategic argument for promoting SIENA was made by some of the stakeholders: as **Europol is seen as the information hub**, it would also make sense to use SIENA as default channel. This would be politically consistent. In addition, it was mentioned during the expert panel that the use of SIENA simplifies information-sharing with Europol, which is another reason for further promoting the use of SIENA.

Based on our research, **binding rules on the choice of channels in general and the use of SIENA in particular** are not considered feasible at this point. It is however seen as feasible to promote SIENA further so that it becomes de facto the default channel.

As an additional measure to establish a further connection between the different channels, a proposal for an **Information Exchange Platform** has been developed by Europol and presented to the DAPIX working group. The proposal includes developing a common information exchange platform (IXP) (i.e. a portal with help functions, guidelines and also an operational multi-query function for all relevant EU systems). This was welcomed by the Council in its Conclusions on EIXM[170], where it invites Europol to continue working on the development of this platform. The further work on this tool has temporarily been put on hold, mainly because of resource issues. However, it is planned to integrate certain of the IXP ideas, such as the concurrent search in different databases, in the follow-up project to the UMF II (see section 4.2.4).

4.2.2.5 Conclusions

The choice of channel currently depends on many factors, which are not consistent across and not even within Member States. In most Member States, the decision on the choice of channel is made solely by the SPOC officers.

Manuals and instructions to guide SPOC officers exist at EU level and in most Member States. However, national instructions are not always coherent with the EU Guidelines, they are not always up-to-date and used to a limited extent even where they exist on national level. Thus, the choice of channel is often assessed more on a case-by-case basis. While official guidelines are taken into account to an extent, personal considerations, including preferences for a certain channel, also play a major role. There are obstacles to the process of adopting standards that are more binding, because in some Member States the prevailing attitude is to leave the choice open for the officers to ensure flexibility. The unstructured choice of channels causes complexity for the SPOC and generates risks related to the quality of the data. Sending requests via more than one channel causes problems in Member States that do not have a single case management system.

In terms of the actual use of the different channels, the Europol channel is by many wrongly seen to be confined to the Europol mandate. The Interpol channel is also currently used in many cases when only EU Member States are concerned. It is popular among many of the stakeholders consulted, because it is perceived to be very convenient to use since messages can be sent in free text format and it is well-accepted because it has existed for a long time. The SIRENE channel and the SIS II network are still used in some Member States for exchanges under Article 39 CISA although legally not

[169] In particular, he referred to the principle of purpose limitation and noted that an increase in the use of SIENA should not widen its functions beyond its original purpose. See the Opinion of the European Data Protection Supervisor on the EIXM Communication, p. 8. (https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-04-29_EIXM_EN.pdf)

[170] C.f. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/137402.pdf.

permissible anymore. Informal communication plays an important role but is in most cases accompanied or followed-up by formal requests. PCCCs are generally appreciated for complex cases. There seem to be a few instances where PCCCs are used to circumvent the SPOC.

SIENA is currently used in most Member States, but to a different extent. In many Member States, SIENA is only available in the ENU. A few Member States have started or are planning to make SIENA available to a wider circle of users. Only a few Member States have started to promote SIENA as the main channel for EU information exchange. There are still several hurdles to using SIENA, notably the lack of 24/7 availability in the Member States, the fact that SIENA is in most Member States not yet connected to the case management system, as well as low awareness of and scepticism about SIENA. Europol is working on improving SIENA and is offering support to Member States, for example in connecting SIENA to the case management system.

A proposal for an Information Exchange Platform has been developed by Europol and presented to the DAPIX working group, but the work has been put on hold. It is envisaged that elements of this concept will be implemented in a follow-up project to UMF II.

4.2.2.6 Recommendations

In general terms, the findings of this study indicate that it is imperative for there to be increased coherence in the different approaches used for the choice of channel. In this context, we consider that SIENA suggests itself as suitable for further promotion as the default channel for SFD and Prüm follow-ups to ensure consistency. Yet, this is not feasible based on the status quo. A number of pre-conditions must be met, which need to be tackled by several actors.

- It is considered relevant that directives on the choice of channel, based on the SPOC Guidelines and in line with EIXM, are available at national level. These need to be kept up-to-date and officers need to be made aware of these. This could be done, for example, as a general training session for SPOC officers on the choice of channel, where SPOC officers are reminded of the general principles and referred to the existing guidelines.
- With a view to promoting SIENA as the default channel for SFD and Prüm follow-ups, it would be useful for there to be an endorsement of the SIENA Roadmap prepared by HENU, which sets out the specific steps needed towards increasing the use of SIENA. The following pre-conditions for an increased use of SIENA are deemed particularly relevant on the basis of the findings of this study:
    - SIENA should be made as user-friendly as possible based on the work Europol has carried out already in identifying the needs for improvements.
    - It should be ensured that SPOCs facilitate the use of all channels on a 24/7 basis, including SIENA, in line with the recommendations on the SPOCs. With a view to promoting SIENA, it is of particular relevance that a case management system exists that can be connected to the SIENA web service. This way, 24/7 availability can be ensured because the current 24/7 services would have access to SIENA. In addition, it could be ensured that no intermediate steps are needed to convert SIENA messages to the format used in the national case management system. Europol provides support in this regard.
    - It is considered necessary to raise awareness about the use and benefits of SIENA and to offer increased training about SIENA (cf. also section 4.3.1.3).

- A target date should be defined by which the migration from existing procedures must have been accomplished.

- With a view to promoting more direct exchange of information without losing information, it is considered useful that the process of making SIENA available to a broader circle of end-users be continued, while examining technical solutions that facilitate routing messages via the SPOC. In addition, the use of SIENA by PCCCs should be promoted. Some Member States have started or are planning to make SIENA available to officers in the field. It would be necessary to exchange good practices in this regard.

- To ensure consistency, there should be an examination of how existing instruments need to be amended, and the choice of channels and the use of SIENA should be included in this (cf. the recommendations on the SFD and Prüm).

4.2.3 The use of instruments to exchange data from national police records

Information from national police records that is currently not available via existing EU-level tools (e.g. SIS II, Prüm or EIS) is usually handled by National Contact Points (NCPs), following requests from other Member States. The Member State making the request is notified whether the information they are seeking is available, leading to a subsequent formal request for it.

The efficiency of this approach has been questioned, for example, in a note from the French and Finnish delegations to the Working Group on Information Exchange and Data Protection (DAPIX) in October 2012.[171] In the note it was estimated that 65% of the requests are not answered at all. Furthermore, they stated that in view of the "considerable amount of manual work involved, it seems plausible that a lot of possible requests are not sent at all in order to avoid unnecessary efforts in the requested Member States".

In order to improve the efficiency, a proposal was raised in the DAPIX working group, that a new system, named EPRIS (European Police Records Index System), be considered. The working group endorsed the proposal and a study was initiated in 2011. The study showed that there are several existing systems that could serve the business needs and purposes intended for EPRIS.[172] However, there is no single system at the moment that addresses the needs in a comprehensive manner. The Commission, in the EIXM Communication issued in December the same year, concluded that the development of a dedicated EPRIS is not justified: *"In line with the cost-effectiveness principle, the Commission considers that creating an EPRIS is currently not justified given that existing instruments and tools, which could serve this purpose partly or fully through better or intensified use, are not fully used. This concerns in particular the Europol Information System (uploading relevant data and extending access at national level), SIS II (increasing use of relevant alerts on persons or vehicles for checks for the purposes of prosecuting criminal offences and preventing threats to public security), SIENA (further developing access at national level, interlinking with national systems and automating tasks where appropriate), and Prüm (full implementation to improve identification of criminals acting in different Member States)."*

On this basis, France proposed to take the lead on a project to automate the searching of national police databases. Europol and a number of other Member States have also expressed an interest in the project, 'Automation of the Data Exchange Process' (ADEP), which seeks to enhance information exchange by automation of current manual procedures for querying.

4.2.3.1 Issues related to implementation of the proposed solutions

The proposals for EPRIS and ADEP raise two basic questions:

1. What is the exact definition of "police record" both in relation to the law enforcement life cycle and to the type of criminality?
2. Could the existing EU systems/instruments be used more extensively to reach the level of exchange that these proposals are aiming for?

The answer to the second question depends to a large extent on the exact definition of what a "police record" is. The EPRIS study defines "police records" as: *"A 'Police Record' shall mean any information available in the national register or registers recording data of competent authorities, for the prevention, detection, investigation and prosecution of criminal offences."*

---

[171] Document no. 14944/12 of 15 October 2012; DAPIX 129.

[172] C.f. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/docs/epris-final_report_en.pdf.

This broad definition was made after consultation with the Member States, which according to the study did not want to put too many constraints on the definition. This definition would in principle encompass all the data that is already exchanged in the existing instruments at EU level. It therefore it does not actually serve very well as a definition for explaining the information need that is the basis for the proposals of EPRIS and ADEP.

A survey made in 2005 by the MDG (the Multidisciplinary Group on Organised Crime established by the Council) investigated what competence the police had in using various types of data autonomously. It is clear from the summary of this investigation that, even if a majority have common or similar rules, many Member States differ quite starkly as to what the police authorities are entitled to use autonomously and which data judicial authorities and judicial decisions are needed. This fact must also be taken into account when looking at what data could be further exchanged, how this data is defined and what means to use for the information exchange.

Interviewees in Member States, but also stakeholders at central EU level, stated that there is a need for further information exchange and that the ADEP proposal is interesting. The expert panel was also of the opinion that there is a need for further information exchange, but preferred to discuss alternative solutions, using existing systems, instead of aiming for ADEP.

Some experts claim, in this context, that certain types of data are of common interest in particular, but are often not shared. Examples mentioned relate to background data on terrorists and data on crimes that are seen as minor, but behind which there is often an organisation. This relates to cases that on their own do not merit the sharing of information (e.g. burglary of houses and shops, crimes impacting tourists and travellers on their way through Europe, vehicle theft). However if this kind of data were to be shared and analysed, it might show that these petty crimes are related to organised groups, who are often mobile and travelling around Europe. In close relationship with this kind of criminality, there could also be cases of drug smuggling and trafficking. With a solution like ADEP where indexes of data from each Member State could be searched, this kind of data would also be found and could be correlated with to other data and reveal organised crime that is not visible at first sight.

How to implement a solution like ADEP was a topic brought up by a majority of those interviewed, both in Member States and at meetings with other actors (i.e. Council, DG Home, EP, EDPS, Interpol, Europol, Frontex, expert panel meeting). A number of potential issues and problems linked to the implementation were mentioned, as follows:

- **Quality of the data registered**. There is no doubt in general on the quality of the source data in Member States databases. The concern relates mainly related to differences in procedures and judicial contexts. These differences could lead to difficulties in the interpretation and use of the data by the Member State requesting the data.
- **Legal basis used to capture/register the data**. There is a problem in ensuring, for any proposed new exchange of information, that the data received has been registered in circumstances and with procedures that are acceptable for the receiving Member State, as potential user of the data. This can be seen as a problem with differences in legislation or as a lack of information about the practical circumstances/procedures when registering the data. The latter would be necessary to enable the receiving Member State to assess if and how the data can be used.
- **Understanding of the data.** Language, differences in culture and organisation, differences in procedures and in legislation, etc. can make the understanding and interpretation of the data difficult when exchanging information.
- **Legal basis for using the data received.** When the receiving Member States, in investigations and prosecutions, want to use the data, there is a need for a clear legal basis on how to act, and what is permissible. This concern relates to the difficulties in establishing common legal

instructions for the whole system and for all users. Depending on the solution found, it can also relate to the complexity in carrying out the necessary bilateral agreements/consultations on a case-by-case basis after a hit.

- **Differences in national laws.** A number of the points mentioned above stem from the fact that national legislation is not harmonised at EU level when it comes to the collection and use of this kind of data.

Concerns are frequently raised about the technical feasibility of building a system containing national indexes to be searched by a central or commonly available component by all Member States. This does not mean that it would be impossible, but rather that there would be risks related to complexity, data protection, time and budget. Moreover, a new system is in itself no guarantee of extended usage of the related data, as can be seen from the example of EIS.

4.2.3.2 Using existing solutions for exended information exchange

A majority of the persons and organisations involved in the study mentioned that possible extended use of existing EU instruments could address the need for further information exchange. This is also one of the primary conclusions of the study on EPRIS in 2012: it should be possible to cover the business needs forming the basis of EPRIS should be possible to cover by using existing systems.

The most common view is that, before looking more in detail at ADEP, the Commission should consider first developing existing EU instruments to provide for extended information exchange. This view is also in line with the general recommendation of the EIXM communication of making the most of using existing instruments and tools before creating new ones. During our fieldwork in the Member States, police officers considered that there are too many, sometimes overlapping, instruments and tools. It makes the exchange of information complex.

When mentioning alternatives to the creation of ADEP, the systems most often mentioned were SIS II, ECRIS and EIS. Each does contain data that could be considered to be part of what is referred to as "police records".

The EIXM study focused on looking at an **extended use of the EIS as an alternative to ADEP**. It is clear that many of those interviewed, and stakeholders on central level, and the expert panel, think that EIS has a potential for extended usage. According to information provided at a meeting with Europol, their internal analysis points to that the potential for number of records in EIS to go from something over 200 000 at present to more than 5 million. The finding on **obstacles** to an extended use of EIS based on interviews and meetings with Member States and stakeholders are:

- **The volume of data is too low**. The fact that EIS has quite low volumes of data makes Member States and the relevant organisations hesitant about putting efforts into feeding EIS more extensively. The reasons why there is not more data in EIS are related to the points below.
- **Registration is possible only if there is an impact on two or more Member States**. This rule is seen as relevant when it comes to data registered for analysis. Data related to cross- border checks is seen as a different case and the existing rule on "two or more MS" is considered too strict for these cases.
- **Security classification**. The high security classification makes it quite difficult to enable access to EIS for field officers. In many Member States, only the ENU and/or the SPOC has access to EIS. This is considered to make EIS less useful in operations and hence it is less attractive for Member States to share data via EIS.

- **EIS does not reach end-users in the field**. The end-users of EIS are often limited to ENUs/SPOCs, as mentioned above. This is partly due to security reasons but also to organisational and technical constraints.
- **Data is registered only in relation to serious organised crimes**. Petty theft and minor crimes, that could be part of organised crime, are not inserted. As mentioned in relation to ADEP, minor crimes, especially when appearing frequently in specific areas, could be an indication of the existences of organised crime. This is not visible until the data is shared and the same persons, cars, objects or behaviour (i.e. modus operandi) are seen by other Member States.
- **Rules on the use of EIS are not clear**. The use of EIS seems to be different among Member States, and interviewees and experts asked for clearer rules on the use of EIS.

4.2.3.3 Conclusions

There is seemingly a business need within the law enforcement area for extended sharing of information within the EU. This relates to data that is not currently shared, mainly since it does not fall under the categories of existing systems (e.g. petty crime) but where most of those interviewed see an added value that will only be realised once the data is shared.

There is a widespread view, however, that a solution for this business need should be sought among the existing instruments, for instance EIS, and EIS could be used to a much larger extent. The main obstacles to this extension are the rules for entering data in EIS, the limited user community and the fact that EIS data is normally not easily accessible on a larger scale in operational police work. This also leads to a vicious circle where the volumes of data in EIS are too small for Member States to think it is worthwhile investing in resources and solutions for making increased use of it.

SIS II, ECRIS and Prüm were also mentioned as existing instruments that could potentially cover part of the business needs expressed.

EPRIS and ADEP are proposals for solutions that would fulfil the business needs mentioned above. In general it is felt that it would be interesting to pursue these proposals further. The interviewees did raise concerns about the implementation of the proposals, for instance regarding the quite vague definition of "police records", which basically could be interpreted as covering all types of data already shared via existing instruments. The quality of data and the ability to share data under using different legislations were other concerns raised.

4.2.3.4 Recommendations

In order to address the findings of the study, an action plan could be drawn up. This would focus on extended use of EIS, SIS II, Prüm and ECRIS – with the aim of covering the information needs that are the underlying reasons of the EPRIS/ADEP proposals. The action plan could contain, as examples:

- Activities for creating a clear, detailed and unambiguous definition of the concept of "police record", the term used in the proposal of EPRIS/ADEP. The definition of "police record" in the EPRIS study could be seen as including all kind of data in existing EU instruments, but this new definition should look at which parts of the crime lifecycle and what type of crime are covered by the existing systems. As a result the concept of "police records", in the context of EPRIS and ADEP, could be narrowed down to mainly cover any existing gap.

- The proposed new regulation for Europol[173] supports a more flexible architecture, to cater for extended information exchange. In addition to a more flexible architecture it could be of interest to include activities in the plan that look at changes in the use of EIS. These changes would concern the rules for entering data for the purpose of cross-border checks, including the rule that entering data requires that at least two Member States have to be impacted by the case and the rules for the types of crime entered (e.g. petty crimes could also be entered in order to find out if these are part of a wider, organised, context). This would be likely to increase the volumes in the EIS and also make it more attractive to use the system.
- Assessment activities resulting in, potentially, proposals for implementation of different security levels for access to EIS, to be applied for cases related to cross-border checks. This would support the ability to create a larger user community in Member States, which in itself could generate better use of the EIS.
- Activities for promoting a wider use of the EIS. This could include information campaigns within Member States, in cooperation with Europol and supported by the Commission. It could also includ support in using the automated data loaders in all Member States, which could extend the amount of data shared.
- Activities for investigation of a potentially wider use of SIS II and/or Prüm and/or ECRIS to partly contribute to fulfilling the information needs expressed.
- Continued activities related to the proposal for ADEP. A detailed analysis of the ADEP proposal should clarify to what extent this proposal could meet the expectations of Member States. It should encompass data protection aspects, the specification of which data Member States are actually willing to share via indexes, how to ensure a sufficient level of data quality, how the EIS could be integrated to ensure complementarity/ avoid duplication, and how SIENA and UMF could be used within ADEP.

[173] On the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA - COM(2013) 173 final

4.2.4 Technical developments beyond UMF II

The term "interoperability" emerged first in the United States in the 1970s, in the domain of national security, a natural domain for public intervention. It only later began to be commonly used in Europe. The first instance of its use by the EU appears to be in the 1991 directive on software copyright. Today, it has become central to the implementation of the Digital Agenda for Europe[174], with several of the chapters mentioning it. The EU has been promoting interoperability since the 1990's. IDA[175] was a pioneer programme promoting interoperability in public administrations by facilitating the transition from paper-based to digital exchanges. From 1999, IDA II paved the way for the IDABC[176] programme launched in 2004 to promote interoperability in the delivery of pan-European e-government Services for public administrations, business and citizens (PEGS – now known as cross-border digital services). IDABC was the first EU programme to envisage a European interoperability policy. IDABC gave the EU its very first conceptual framework for moving forward on interoperability, the European Interoperability Framework (EIF) version 1.0 released in 2004. This framework was later updated, in 2010, under the ISA programme (2010-2015)[177], the successor to IDABC.

Yet, despite interoperability having become a fairly usual term, even today many people think of it as a purely technical concept (because of its origins[178] and because of the nature of the term). However, the scope is broad, as the EIF makes clear. It is "the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems." Thus, interoperability goes beyond technology. It functions at the several levels found in the EIF:

- Legal interoperability: alignment of legislation across Member States;
- Organisational interoperability: alignment of business processes across different organisations;
- Semantic interoperability: alignment of the (precise) meaning of information which can be preserved and understood by all parties; and
- Technical interoperability: alignment of interface specifications, interconnection services, data integration services, data presentation and exchange, etc.

4.2.4.1 Development of the UMF standard

All of the above levels are valid for the standard developed explicitly for police information exchange at EU level, called UMF (Universal Message Format). As the name implies, this refers to a common framework for the structured, cross-border information exchange between law enforcement authorities and/or organisations. UMF defines a common vocabulary and logical structures for commonly exchanged information (e.g. persons, offences, etc.). A framework of semantic interoperability has been developed in the course of the UMF II Programme. The programme is

[174] For more information about the Digital Agenda: http://ec.europa.eu/digital-agenda/.
[175] For more information about IDA see: http://europa.eu/legislation_summaries/information_society/strategies/l24147a_en.htm.
[176] For more information about IDABC see: http://ec.europa.eu/idabc/en/chapter/3.html.
[177] Led by DIGIT, ISA supports effective electronic cross-border and cross-sector interaction between public administrations in Europe. Public administrations are the direct beneficiaries, businesses and citizens are indirect beneficiaries. A key element of ISA is promotion of interoperability through the share and reuse of existing eGovernment solutions to produce ICT systems which enable smooth implementation of EU policies.
[178] This is reflected in one of the most cited definitions of interoperability by (IEEE 1990) which characterises interoperability as "the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

executed under auspices of Council Working Party on Data Protection and Information Exchange (DAPIX), co-financed by the European Commission, and coordinated by Europol.

In the EIXM Communication, the Commission made the following recommendation:

Europol and Member States are invited to:

- Continue development of the UMF standard

The specification of UMF II was introduced in May 2014. At present only a few Member States have implemented this standard, and only to a limited extent. Member States using SIENA, for Prüm and the Swedish Framework decision, do sometimes use UMF II attachments, which are built in as features of the SIENA tool.

A problem for Member States that have introduced UMF II is that Member States receiving the request most often cannot send the answer using UMF II. This limits the usefulness for the Member States that are front-runners in implementing UMF II and it also hampers willingness to introduce UMF in general.

There was a consensus among everyone involved in the study, when discussing UMF, that a common format for information exchange is necessary and also brings added value in terms of better quality assurance, interpretation of the data and harmonisation of data exchanged.

A majority of Member States mentioned that they are following with interest the development of UMF II into UMF III, as the next extension of the UMF standard, and want to participate at some stage. Some Member States say that they will actively participate in the UMF III project.

There is no obligation to use UMF in relation information exchange. The interest in using it builds therefore on the benefits it can provide, how much it is used by Member States in general and whether it is integrated in tools used (e.g. SIENA) and thus utilised as part of using the tool.

4.2.4.2 Conclusions

UMF is seen as essential for existing and future extensions of information exchange, in particular for instruments where other standards do not yet exist. The implementation of UMF II is making rather slow progress, mainly due to budgetary issues but also due to the short time that has elapsed since the standard was launched. There is quite high interest among Member States to proceed with implementing it and also to follow the creation of UMF III, which is the next version of UMF, extending its functions. UMF is implemented in SIENA and can be used for Prüm and SFD. This feature is today only used by the Member States using SIENA, and even then not in all cases. A number of interviewees and the expert panel regretted that UMF is currently not mandatory for certain types of information exchange, to make sure that it is used.

4.2.4.3 Recommendations

- A recommended way forward is to ensure that UMF would be a built-in feature of any common EU tools used, as it is in SIENA. This facilitates the use of UMF and considerably limits the work and investments needed in Member States to implement UMF
- Consideration could be given to taking measures to make SIENA the standard tool for Prüm follow-up, SFD and any other information exchange where the choice of channel or tool is not regulated in the instruments.

- The two recommendations above would, in principle, ensure that UMF is used in all information exchange where it is currently feasible within the legal framework. Investments on the Member State side would be limited and the use of UMF would be maximised.
- If the recommendations above are not achievable, the following activities could be considered:
    - Reflection on further measures to make UMF the mandatory standard for Prüm, SFD and other information exchanges where the format of the data exchanged is not regulated.
    - Member States should implement UMF via automated functions, feeding data from the national systems or central systems into the defined structure.
    - An overall plan for UMF implementation in Member States and at EU level should be drawn up.
    - Support to Member States in the implementation of UMF (e.g. a Helpdesk function) and specific funding to Member States for the purpose of developing the necessary function for implementing UMF.
- The IXP concept contains many good ideas, in particular related to concurrent searches and data insertion that could be re-used when developing UMF further.

4.3 Horizontal challenges of EIXM

4.3.1 Training measures

Article 87 of the TFEU on police cooperation provides for measures for the support for the training of staff, and cooperation on the exchange of staff, on equipment and on research into crime-detection should be established with regard to police cooperation.

A number of **different EU-level actors** are active in this area and thereby complement the offer of national actors,[179], such as police academies and law enforcement authorities. The EU entities playing a role include, in particular, CEPOL and Europol.

As stated in the Council Decision on the establishment of **CEPOL**[180], CEPOL's tasks include the training of senior police officers of the Member States by bringing together the national training institutes. There is a special focus on the training of police officers playing a key role in combating cross-border crime (Article 7c). CEPOL's task is also to facilitate relevant exchanges and secondments of police officers in the context of training. One relevant component of CEPOL's training activities is e-learning, which supports traditional methods and ensures a broad reach of the training measures.[181]

Europol plays an important role in training. It is Europol's task to pioneer new techniques as well as facilitate knowledge-sharing and quality training for law enforcement authorities' staff in the Member States. This is also reflected in the Council Decision on the establishment of Europol[182]: Article 5 stipulates that Europol should assist Member States through support, advice and research in relation to the training of members of their competent authorities, where appropriate in cooperation with CEPOL. Furthermore, Europol provides a helpdesk on the information exchange provisions of the Prüm Decisions that focuses on practical problems encountered by Member States' law enforcement officials.[183]

Other institutions in the area of judicial cooperation between Member States may also play a role in the training of staff in the area of police cooperation. These include Frontex, Eurojust, the EU Agency for large scale IT systems (EU-LISA), the European Judicial Network; and the European Judicial Training Network.

In the EIXM Communication the Commission acknowledged the importance of providing high quality training and invited Member States to:

- Ensure that all law enforcement officers receive appropriate training on cross-border information exchange;
- Organise exchanges of SPOC staff.

The Commission indicated that it would:

- Ensure that the European Law Enforcement Training Scheme includes training on cross-border information exchange.

---

[179] This was also noted in the Communication Establishing a European Law Enforcement Training Scheme (LETS), COM(2013) 172 final (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0172:FIN:EN:PDF).
[180] Council Decision 2005/681/JHA of 20 September 2005 establishing the European Police College (CEPOL) and repealing Decision 2000/820/JHA, see: https://www.cepol.europa.eu/fileadmin/website/About_CEPOL/2005681jha.pdf.
[181] C.f. https://www.cepol.europa.eu/index.php?id=e-learning.
[182] Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), see: https://www.europol.europa.eu/sites/default/files/council_decision.pdf.
[183] C.f. *Europol Review 2012* (https://www.europol.europa.eu/sites/default/files/publications/europolreview2012_0.pdf).

4.3.1.1 The developments with respect to the training landscape

With a view to streamlining and improving the existing offer, the Commission issued the Communication *Establishing a European Law Enforcement Training Scheme* **(LETS Communication)**[184] shortly after adoption of the EIXM Communication. The LETS Communication emphasises the importance of appropriate training on law enforcement cooperation instruments for law enforcement officials of all ranks. **Improving knowledge of EU instruments for information exchange and the EU dimension of day-to-day policing is considered as one of the needs**. To improve and streamline the current offer, the LETS Communication suggests developing four strands of training, three of which are relevant in the context of this study as they cover aspects related to cross-border information exchange:

- *Strand 1 – Basic knowledge of the EU dimension of Law Enforcement:* This strand suggests that all EU law enforcement officials should have a basic understanding of the EU instruments that are relevant in the context of cross-border law enforcement cooperation, including on the use of EU information management tools and channels. In this context, the Commission asks CEPOL (in cooperation with Member States and Frontex) to propose a standard EU level of knowledge and skills in these fields for all law enforcement officials.
- *Strand 2 – Effective bilateral and regional cooperation*: This strand aims to ensure that law enforcement officers have sufficient knowledge of the relevant EU and bilateral instruments as well as knowledge of languages and cultural sensitivity.
- *Strand 3 – EU thematic policing specialism*: This strand aims to ensure high quality training on the crimes that are considered priorities by the EU, including trafficking in human beings or drugs, and cybercrime. Cross-border cooperation should be covered, where relevant, as part of this training. CEPOL is asked to prepare a gap analysis and develop training on that basis, together with the network of national police academies.
- *Strand 4 – Civilian missions and capacity-building in third countries*: This strand is beyond the scope of this study.

In addition, the Communication sets general goals including e.g. quality assurance. The implementation of LETS requires the cooperation of several actors, in particular EU agencies, national academies and the European Commission. The Training Scheme is also generally welcomed by nine relevant agencies[185] as a means to improve cross-border law enforcement cooperation.[186]

The LETS Communication was **welcomed by some of the stakeholders consulted for this study as a step forward**. It was often stressed that cross-border information exchange can be improved through appropriate training activities. Some interviewees highlighted the fact that coordinated measures at the EU level are welcome. For example, one interviewee indicated that the proposed European Law Enforcement Training Scheme and its aim of concentrating efforts on the basic knowledge of the EU dimension of law enforcement, including the use of EU information management tools and channels, such as the Swedish Initiative and the Schengen Information System.

However, **implementation of the LETS is not moving as rapidly as hoped**. There are still consultations about the roles the different actors will play in this regard and how their activities will be financed. As explained above, the plan is for CEPOL to play a central role. According to CEPOL, however, the

[184] COM(2013) 172 final (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0172:FIN:EN:PDF).
[185] Eurojust, Frontex, eu-LISA, EASO (European Asylum Support Office), EIGE (European Institute for Gender Equality), EMCDDA (European Monitoring Centre for Drugs and Drugs Addiction), CEPOL, Europol, FRA.
[186] C.f. https://www.cepol.europa.eu/media/news/content/20131127/eu-agencies-discuss-european-law-enforcement-training-scheme-european.

resources it is granted do not allow it to take on such additional tasks.[187] In 2014, CEPOL's work was complicated by the move from Bramshill to Budapest. In addition, there are on-going discussions about a new legal framework for CEPOL. The adoption of a new legal framework may provide a new basis for the participation of CEPOL in the activities referred to above. Moreover, CEPOL has nevertheless aligned its Work Programme and training activities as far as possible with the LETS, with a focus on Strands 3 and 4.[188] In general terms, CEPOL considers itself as one of the key actors in the context of EU law enforcement training and it is intended that it should play a key role in implementing the principles of the training model.[189]

In general terms, the interviewees and participants in the expert panel acknowledged the efforts by different actors at the national and EU level. Yet, interviewees and participants in the expert panel identified **shortcomings in relation to the current offer** at national and EU level. In particular, there are currently **gaps in the overall offer and the quality of delivered training is not always sufficient**.[190] The previous sections have illustrated aspects of this in that law enforcement officers are currently not sufficiently aware, for example, of the meaning of the SFD (cf. section 4.1.1.4) or the functions of SIENA (cf. section 4.2.2.3), as well as competencies that are currently not sufficiently developed, such as language (cf. section 4.3.2.3). This may point to gaps in the training offer. In terms of quality, the stakeholders consulted indicated that the standard of national training is not yet consistent.

The next sections discuss the current landscape and the gap identified gaps in relation to three categories of training:

- Initial training;
- Onboarding for SPOC officers; and
- On-going training.

a) Initial training

The stakeholders consulted generally considered that initial training is the responsibility of the Member States. Although there are some cooperation programmes, the current offer is mainly based on national efforts.

It was recognised by all stakeholders consulted that it is very important that students in the law enforcement academies receive training about the relevant instruments for law enforcement information exchange. It is recognised that freshmen need to learn about the institutions that are relevant in the context of cross-border cooperation, including in particular the national SPOC, as well as possibilities for exchanging information in cross-border cases. It was, however, pointed out during the expert panel that the possibilities for teaching this subject to freshmen on a theoretical basis are limited. Therefore, policy makers and managers at law enforcement authorities consider solid basic training necessary, which can serve to present an overview and which needs to be deepened later on. It was also noted that practical training, e.g. on the basis of typical cases, is considered as most useful.

---

[187] According to the *CEPOL Work Programme 2014*, the ""zero" growth environment and proposed resources cuts pose significant challenge to build upon achievements and in some cases even impossibility to retain the achieved." It is specified that there is no additional budget to carry out the tasks identified in the LETS Communication (p. 7). (https://www.cepol.europa.eu/sites/default/files/work-programme-2014.pdf)

[188] See *CEPOL Work Programme 2014* (https://www.cepol.europa.eu/sites/default/files/work-programme-2014.pdf) and CEPOL Training Catalogue 2014 (https://www.cepol.europa.eu/sites/default/files/training-catalogue-2014.pdf).

[189] Cf. *CEPOL Work Programme 2013* (https://www.cepol.europa.eu/sites/default/files/WP_2013.pdf)

[190] See also: *Mapping of Law Enforcement Training in the European Union*, CEPOL 2012 (a summary is available at: https://enet.cepol.europa.eu/fileadmin/documents/LETS/LETS_Management_Summary.pdf); Communication Establishing a European Law Enforcement Training Scheme (LETS), COM(2013) 172 final (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0172:FIN:EN:PDF)

The training that is provided at national police academies does not always fulfil these criteria. Several shortcomings have been identified. They are discussed in the following paragraphs

In a few Member States, **that there is no assurance of training on cross-border aspects of law enforcement (for all students)**. Indeed, only 44% of policy makers (i.e. 20 out of 45) indicated in our web-based survey that curricula for officers at the academy include training on cross-border information exchange. This is confirmed by a mapping carried out by CEPOL. The mapping indicated that at least one law enforcement authority in most Member States indicated that initial training covers European cross-border law enforcement cooperation. However, in four Member State no law enforcement authority indicated that this is the case.[191] In some Member States, **not all students receive basic training on international information exchange in the police academy**. For example, in one Member State, there are different training streams, one for students striving to become high ranking officers, the other for low ranking officers. In the stream for high ranking officers, there are general courses relating to international police cooperation. However, in the academy for lower rank police officers no such training is offered according to one of the interviewees.

During the interviews, most stakeholders in ministries and law enforcement authorities indicated that there is some training in this regard but that the **offer is too small**. For example, officers from some countries noted that they only had a short session on this topic and that the information provided was not sufficiently detailed.[192] Based on the input CEPOL received from the participating law enforcement authorities, there are great variations in the duration of initial training, namely between one and 30 months. Stakeholders consulted for this study also pointed out that, where training is short, not all relevant topics are covered. This is also supported by the findings of CEPOL's mapping, which shows that the different topics are not covered to an equal extent[193]:

- Schengen Acquis (in 36 out of 42 law enforcement authorities);
- Prüm Decisions (in 21 out of 42 law enforcement authorities); and
- SFD (in 12 out of 42 law enforcement authorities).

Some interviewees regretted that the training offered at the police academies is **too theoretical**. In our web-based survey, field officers and SPOC officers ranked basic training provided at the police academy lowest compared to other types of training.[194]

Based on these shortcomings, some stakeholders specifically argued that the **awareness of field officers of the possibilities for exchanging information is too low because the topic is not sufficiently covered at the police academy**. Some noted that there have already been improvements in the past few years. However, as CEPOL points out in its Work Programme 2014, many training institutes in the Member States are currently affected by financial cuts.[195]

---

[191] No law enforcement authority In Bulgaria, Czech Republic, Romania or the UK indicated that initial training covers European cross-border law enforcement cooperation. There were some additional exceptions within the Member State law enforcement authorities: in Germany (for customs and one state police), Ireland (for the national police and for the customs), Italy (for one of the national police agencies), Latvia (for customs and border), Malta, Poland, Slovenia and Slovakia (for customs), and Portugal (for one of the national police agencies and for customs). Mapping of Law Enforcement Training in the European Union, CEPOL 2012 (a summary is available at: https://enet.cepol.europa.eu/fileadmin/documents/LETS/LETS_Management_Summary.pdf), p. 13.

[192] For example, one interviewee reported that he had 10 hours of training and then an exam on international cooperation.

[193] Mapping of Law Enforcement Training in the European Union, CEPOL 2012 (a summary is available at: https://enet.cepol.europa.eu/fileadmin/documents/LETS/LETS_Management_Summary.pdf), pp. 17-18.

[194] Training at the academy was ranked 2.8 out of 5 by field officers and 3.07 out of 5 by SPOC officers. It is noted that SPOC officers generally applied a higher rating to all types of training listed compared to field officers.

[195] *CEPOL Work Programme 2014* (https://www.cepol.europa.eu/sites/default/files/work-programme-2014.pdf), p. 7.

b) Onboarding for SPOC officers

Taking into consideration the various structures of the SPOC, it is clear that onboarding programmes (as well as information needs for SPOC officers) vary across Member States. While this was not discussed in all the interviews, some interviewees mentioned specifically that they saw room for improvement in this respect.

In particular, a few interviewees pointed out that in some Member States there is no introductory training for SPOC officers. Rather, new SPOC officers have to start working immediately with some support, e.g. by a tutor or coach who is assigned for a specified period. The possibility of a tutor or coach being assigned was generally considered very helpful. However, it needs to be noted that tutors have to do this job on top of their daily tasks and may not always be accessible.

A few SPOC officers mentioned that they felt overwhelmed at the beginning and would have wished for an induction before they actually had to work on concrete cases. One interviewee also noted that she received a large pile of legislation to read, which was difficult to process.

c) On-going training

Most stakeholders consider on-going training the most important category of training. There is currently a variety of offers at national and EU level based on the inputs received during this study.

The following types of training exist at **national level** for all or some EU Member States:

- Written information (e.g. manuals, guidelines, folders, web pages);
- E-learning;
- Theoretical or practical seminars to deepen the knowledge about international information exchange or to inform the officers of new developments;
- Information sessions by the national SPOC (targeted at field officers); and
- Language training (mostly targeted at SPOC officers).

In addition, Member States make use of different types of training that are offered or **organised together with other Member States or centrally in the EU**:

- Training offered by CEPOL, including webinars;
- Workshops and seminars offered by Europol, e.g. on SIENA;
- Europol roadshows are offered to each Member State;
- SIRENE and SIS II training is organised regularly, by eu-LISA, in cooperation with CEPOL and SIRENE offices;
- Staff exchanges, e.g. funded by EU programmes or organised and financed by the participating Member States (mostly considered relevant for SPOC officers);
- Exchange of practices at conferences, either at EU level or with a group of neighbouring Member States;
- Exchange of practices in the framework of the Europol Platform of Experts (EPE)[196];
- Annual meetings of specific departments organised on a bilateral or multilateral basis;

[196] The EPE facilitates knowledge sharing and communication for experts and practitioners in various subject matters relating to police cooperation. The EPE is accessible to members upon invitation. There are currently about 4000 users. Members include: Law enforcement, Private companies, Academia, as well as other organisations from EU and third countries. C.f. https://www.europol.europa.eu/content/page/europol-platform-experts-1851 as well as *Europol review 2013.*

- Infopolex[197];
- MEPA[198];
- Training offered by international organisations, such as Interpol or the UN.

Some general points can be made with regard to the different types of training.

First, it seems that **there is more EU level training than national offers**. In our web-based survey, 55.6% of policy makers (i.e. 25 out of 45) indicated that continuous training offers include elements on cross-border information exchange; 80% (i.e. 36 out of 45) indicated that their staff participates in training sessions delivered at EU level by CEPOL, SIRENE bureaux, Frontex etc. This was confirmed in the LETS Communication, which reported that the numbers of officers taking part in EU training has been growing, with more than 5 000 enrolled at CEPOL and 3 000 at Frontex in 2012.

Second, **practical training is considered more useful than theoretical**. For example, staff exchanges with hands-on experiences or courses/workshops with practical case examples were considered as highly useful by those consulted.

Third, **while written manuals can be a support to SPOC officers and field officers, they cannot replace training**. One interviewee highlighted the fact that operational staff generally have very little time to read manuals. Therefore, the most relevant information needs to be provided in actual training sessions.

Finally, in some Member States, **there is no overall training plan**. Training is offered on a rather ad hoc basis, depending on availability of staff, staff's personal interests, and possibilities such as CEPOL.

Apart from these general observations, it is acknowledged that the offer and needs of SPOC officers and field officers vary. Therefore, the following paragraphs discuss the existing possibilities for on-going training and perceptions on the quality of the current offer discussed separately for SPOC officers and field officers.

SPOC staff

It is generally recognised by the stakeholders consulted that SPOC staff are in need of specific training.[199] In some Member States, SPOC staff needs to be able to work with all existing channels.

At national level, **ongoing training on international information exchange and related aspects is offered to SPOC staff in all Member States**.

Written information in different forms plays a role in all SPOCs.[200] There are, for example, written updates in the event of any changes[201], as well as manuals focusing e.g. on the use of a specific channel. For instance, in Sweden, the SPOC has manuals for every type of cooperation (SIRENE, Europol, etc.)

---

[197] The Infopolex Coordination Initiative is an ISEC-funded project that was initiated by Hungary. The objective is to support cross-border law enforcement cooperation by analysing the problems and identifying solutions together (http://ec.europa.eu/dgs/home-affairs/financing/fundings/pdf/isec/isec-grants-awarded-2011_en.pdf; Council Document *Outcome of the Infopolex Conference held in Budapest on 28 February – 1 March 2011*, Doc number 8339/11).

[198] The Central European Police Academy (*Mitteleuropäische Polizeiakademie*) - MEPA is a training institution that is based on a cooperation between several countries (AT, CH, CZ, DE, HU , SI, SK) and is supported by EU funding. http://www.mepa.net/Deutsch/Seiten/default.aspx.

[199] See also *Draft SPOC Guidelines for cross-border law enforcement information exchange,* Council Document 10492/14, where it is highlighted that "Staff receives regular training, both about EU and international cooperation mechanisms (i.a. via CEPOL) and about national developments."

[200] The existence of written manuals at national level was discussed in sections 4.1.1 and 4.2.2.1.

[201] Many interviewees pointed to the need to keep up to date with the many changes going on in the framework of international police exchange.

These are updated continuously. There is one manual on the choice of channels, which presents the different types of cases and possible actions on one page. An Austrian interviewee pointed to the usefulness of instructions that have been developed on the basis of questions that were posed in seminars and feedback by participants. There have been efforts to understand and collect the types of questions officers typically have. For the development of Prüm instructions, a biologist was involved as well. Yet, as noted above, although such guidelines on international information exchange and the choice of channel do exist in most Member States, they are not always used, e.g. because they are not regularly updated or police officers are not aware of them. It was regretted by some of the interviewees that helpful manuals are not always available.

E-learning, which would facilitate training at a relatively low cost, is currently used quite efficiently in some Member States (this was mentioned, for example, by interviewees from HU, SE, SI). One example is Slovenia, where officers have to take annual online tests about the various tools. Yet, on the basis of the interviews, there are a number of Member States where e-learning is not offered.

On-going learning through seminars is not offered regularly in all Member States. Indeed, a large part of the ongoing training (or indeed the entirety in some Member States) consists only of on-the-job training or written updates. Thus, many SPOC officers do not benefit from specialised seminars, at least not on a regular basis. Some interviewees from the policy level pointed out that training is often difficult to organise due to a lack of resources. In some Member States there are extensive programmes, e.g. comprised of different modules, including on relevant legal bases and channels available.

Example: Development of a training plan in Lithuania

Recently, a new model for vocational training was introduced in Lithuania. Under this new model, police officers can choose which modules they want to take. One module is, for example, focused on international information exchange. Modules take about 16 hours at once and are organised within a classroom setting, including practical problem-solving exercises. The module on information exchange includes information on different international instruments.

Language training is considered an important area for improvement, as noted in section 4.3.2.3. Most Member States offer specific language training for SPOC officers. For example, in Germany, SPOC officers can attend one language course of 2-3 weeks when joining the SPOC. They can choose between the main Interpol languages, but most choose English. However, many interviewees indicated that the extent of the training is not sufficient. Even where Member States offer two-to-three week language courses, it is very difficult to spare any SPOC officer for this time, which is why the actual use of such courses is limited. In other Member States, language training is provided more on an ad hoc basis and by teachers who do not have sufficient training.

Many officers also make use of **training at EU level**, which is considered very useful for field officers, SPOC staff and law enforcement management positions.

CEPOL (often with trainers from Europol) organises seminars mainly for senior police officers[202] on specific criminal activities and not related to information exchange, but focusing more on serious crime. However, it seems that **not all Member States make use of the training offer that requires the officers to travel**. In our web-based survey, 80% (i.e. 36 out of 45) policy makers from 15 Member States indicated that their law enforcement staff can avail themselves of training sessions delivered at EU level by CEPOL, SIRENE bureaux, Frontex etc. Interviewees from ten Member States specifically

[202] See Article 5 of the CEPOL Decision.

mentioned that they or their colleagues have participated in training offered by CEPOL.[203] Some interviewees explained that only a limited number of officers can go to such training due to budgetary constraints. Moreover, in some Member States it is necessary for officers to go through cumbersome official authorisation procedures to attend training. In addition, most training is provided in English, which potentially excludes a large number of officers.

The **CEPOL webinars** are used in several Member States.[204] Based on our interviews, the webinars are seen as a positive way of carrying out training and were appreciated by most of the SPOC officers who participated. Some interviewees pointed to the efficiency of these webinars, as officers do not have to travel. Of course, participation still depends on the workload, as courses are organised during working hours.

The seminars and awareness-raising events organised by **Europol** are generally appreciated by the participants. They are felt to be very well organised. Some stakeholders wished for more training by Europol to improve faith in Europol and its offer. In addition, some interviewees wished for more training on SIENA.

Exchanges of practice in various forms (e.g. CEPOL conferences, staff exchanges) were seen as highly important by almost all stakeholders consulted.

Staff exchanges to other Member States or to Europol are considered as very helpful by the majority of stakeholders. **Staff exchanges take place in some Member States and are mostly organised on a bilateral basis**. Generally, such exchanges, as well as visits to Europol, are considered very useful in learning more about the relevant procedures as well as in getting to know officers from other Member States. In terms of the length of exchanges, some interviewees felt that even a few days were already useful for getting to know the organisation and colleagues. Longer exchanges bring even more benefits, because it is possible to work together on actual cases. The following benefits were highlighted by SPOC officers, who went on exchanges:

- Getting to know the organisational structures in other Member States helps to understand their behaviour and needs, e.g. which information they need as part of requests, why a reaction might take longer.
- The establishment of personal contacts helps in the handling of cases and can even lead to a more European way of thinking.
- Exchanges to Europol help in understanding Europol's needs and the benefits, and in so doing help increase trust in Europol.
- Language skills can be improved on exchanges.

However, the **number of staff exchanges is limited by financial resources** available to the SPOCs at the national level. In addition, **the utility of exchange programmes is not always acknowledged by senior management**. A few interviewees reported that some managers are critical of the cost-benefit balance, and this is an obstacle. Therefore, some interviewees reported cases where exchange programmes could not be carried out or took place only after long negotiations. A minority even

[203] This is in line with the Commission Impact Assessment on merging the European Police College (Cepol) and the European Police Office (Europol), and implementing a European police training scheme for law enforcement officials, SWD (2013) 98 final (http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2013/swd_2013_0098_en.pdf). Indeed, the Commission indicated that in 2010 only around 13 to 15 Member States were able to send officers to make use of CEPOL training.

[204] This was also acknowledged in the LETS Communication, where it was noted that "new learning methods, such as CEPOL's 'webinars' were used by more than 3 000 participants in 2012".

expressed the feeling that their superiors believe that those who apply for exchange programmes are lazy and do so to avoid actual work.

In addition to exchanges, interviewees mentioned other formats that have brought similar results. For example, there are **annual meetings between the biometrics departments of Austria, Germany, and Switzerland** where every province sends one senior officer. The purpose is mainly to get to know each other. The resonances are positive – personal contacts can help in some situations. For example, if a German federal state were regularly sending information with missing parts, it would be possible to ask a relevant officer personally why this is the case and find solutions. Several interviewees from the law enforcement services wished that there were more opportunities like this.

Finally, some Member States make use of the **training provided by international organisations**, such as the UN or Interpol. However, very few interviewees or respondents to our web-based survey mentioned having participated in such training. One interviewee from Interpol noted that most Interpol training nowadays targets non-EU countries.

It was possible to identify some additional gaps in the current offer for SPOC officers. First, in the area of **dissemination of knowledge acquired on EU training**, there does not seem to be a general strategy in most Member States based on the interviews.[205] In addition, there seems to be a **lack of training on data protection**. None of the stakeholders consulted specifically mentioned that they had participated in such training. This is in line with the mapping carried out by CEPOL: in 2012, there were six Member States that seemed to offer no training on aspects relating to fundamental rights, including data protection.[206]

It was also noted that **specialised training is necessary for officers working in the 24/7 service departments**. These officers typically need to work with all existing channels and need to handle any type of urgent cases directly. For example, one interviewee regretted that these officers need to know about all aspects of information exchange, but are neglected when it comes to training. According to the interviewee, training opportunities are much better developed for specialised investigators, who, for example, can participate in workshops at Europol. The interviewee would be interested in receiving more insights into EU policies.

Field officers

There are different perceptions on the extent to which field officers need to be aware of institutions and mechanisms for international information exchange. The extent to which field officers are actually involved in information exchange depends on national structures. As pointed out previously, the extent to which field officers are involved in information exchange varies.

On this basis, the **training offer for field officers is not as well developed as for SPOC officers**. This was regretted by several interviewees. For example, an interviewee in a managerial position argued that field officers need more information and training, to be able to use the possibility of international information exchange more often and better. Officers currently have difficulties in seeing the full picture. Indeed, in some Member States there is hardly any on-going training about international

[205] This was also noted by the Commission in the Impact Assessment on merging the European Police College (Cepol) and the European Police Office (Europol). *Commission Impact Assessment on merging the European Police College (Cepol) and the European Police Office (Europol) and implementing a European police training scheme for law enforcement officials,* SWD (2013) 98 final (http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2013/swd_2013_0098_en.pdf)

[206] *Mapping of Law Enforcement Training in the European Union*, CEPOL 2012 (a summary is available at: https://enet.cepol.europa.eu/fileadmin/documents/LETS/LETS_Management_Summary.pdf), p. 52.

information exchange in the field. Smaller offices in particular do not have a lot of information available.

Written information targeting field officers exists to an extent. In terms of the existence of **national instructions or manuals for situations in which field officers are confronted in cross-border cases**, 73.6%[207] of the policy makers responding to our web-based survey stated that such instructions/manuals are in place.[208] A slightly lower proportion (65.9%[209]) of the field officers stated that they are aware of these instructions or manuals.

In some Member States **the SPOC is active in providing training and information sessions** to field officers. For example, in Hungary and Sweden (cf. box below) the SPOCs run roadshows to make field officers aware of their offer. There is an absence of such an offer in other Member States. This was specifically wished for by some field officers from Member States, where such an offer currently does not exist. They argued that knowing the procedures of their international police cooperation department would help them in knowing which information they need in order to send a request to another Member State.

Example: Training sessions for field officers offered by the Swedish SPOC

In Sweden, the SPOC offers workshops for field officers with the aim of raising awareness of international aspects of police work, including the SPOC. The national visits, including training in real cases, that the Swedish SPOC made to three regions is an example of hands-on training that really raises interest. In the field visit they sit down with the local officers and look at real cases, find areas where international requests could be made and then show them the concrete results of their request. This hands-on training has proved very popular and has greatly increased the number of requests from the three pilot regions[210]. The plan is to widen this activity to all Swedish regions.

MEPA[211] is made use of by several Member States: Austria, Czech Republic, Germany, Hungary, Slovenia and Slovakia. However, according to the interviewees only a limited number of officers can make use of this training due to budgetary constraints.

Exchanges were by many only considered relevant for SPOC officers. However, there are also examples of field officers who sometimes work on international cases (e.g. field officers focused on drugs) who have been on an exchange. This was considered highly useful by those concerned.

Training on international information exchange is in some cases also **included in topical training**.[212] For example, in Austria there is an annual three-day seminar for case officers working with DNA. International exchange of information is also part of this seminar. In some Member States seminars are offered to criminal officers on a regular basis. Officers can follow courses that are focused on their

[207] Based on 53 responses.
[208] Only one person indicated that no such instructions/manuals exist in his/her Member State, but explained that other ways of making field officers aware of the relevant procedures exist. The rest of the policy makers (24.5%) indicated that they did not know whether relevant instructions or manuals exist.
[209] Based on 170 responses.
[210] In one county the requests to the national SPOC increased from 6 to 76, albeit only a minority were cases that could be forwarded in the process, but it shows the interest and is a positive trend.
[211] The Central European Police Academy Mitteleuropäische Polizeiakademie - MEPA http://www.mepa.net/Deutsch/Seiten/default.aspx.
[212] The LETS Communication suggests that training in crime areas with an EU dimension should also include information about cross-border cooperation.

field of specialisation. Where relevant, these include sessions on international exchange of information. For example Prüm is of relevance for officers who focus on sexual offences.

As noted in section 4.2.2.3, some Member States have started or are planning to make SIENA available to field officers. This creates a **need for strengthened training activities on SIENA**.

Example: training on SIENA in Finland

Training on SIENA is available for investigators in almost all 11 police districts. The aim is to train all of them in SIENA. Field officers can send SIENA requests themselves. They use it smoothly. Europol training material on SIENA has been translated into Finnish and more information added. Seminars are held during which actual case examples are discussed which were used in SIENA by the field officers involved in the specific case.

A specific category of officers that are not stationed in the SPOC are those working at the **PCCCs**. In contrast to field officers, they come in contact with international cases regularly and therefore also need specialised training. Various possibilities for training are available to the officers at the PCCC. Generally, they can make use of existing national offers that are useful to them, e.g. seminars on international information exchange or on analysis and investigation. In addition, there are seminars organised by all PCCCs and annual meetings of all PCCCs. Officers at the PCCC have also benefited from the Europol roadshow and seminars organised by MEPA.

4.3.1.2 Conclusions

There are currently a variety of different actors involved in providing numerous different training courses at national and EU level. While the individual activities have generally been appreciated by participants, the main problem is that there is currently no overarching strategy at national and EU level. Many Member States do not have a training strategy identifying needs and rather offer training on an ad hoc basis. At EU level, there is a Communication on a European Law Enforcement Training Scheme, including aspects of information exchange. It is welcomed by stakeholders as providing a framework to the training activities. However, most of the action points have not been pursued further, mainly due to a lack of resources. Thus, it still needs to be fully implemented.

While the individual activities were generally appreciated by participants, there seems to be seems to be a structural lack of adequate training in EU instruments for law enforcement information sharing. There is a lack of awareness in several subject matters, as highlighted across this report. Specific shortcomings have been identified in relation to initial training at police academies, on-boarding for SPOC officers and on-going training for SPOC and field officers.

Initial training at police academies is so far mainly based on national efforts (although it is included in the LETS). Aspects relating to international police cooperation are currently not covered to a sufficient extent in all national police academies.

In terms of on-boarding for SPOC officers, there is often no induction training, which would facilitate the learning process for new officers.

On-going training is considered to be the most relevant. For SPOC officers, there are various possibilities for developing knowledge and skills. Yet, the following shortcomings have been identified: written instructions are not always updated and not used in all Member States; the potential of e-learning is not fully exploited; face-to-face seminars are rarely offered – in most Member States the focus is on on-the-job training and written updates, and CEPOL's seminars are only attended by law enforcement officers of about half of the Member States; Europol training is appreciated, but additional training is necessary on some aspects; staff exchanges are generally seen as highly useful,

but are still limited by financial constraints or managerial doubts about their usefulness; language training is not available widely enough in all Member States. Additional gaps are a lack of strategies on disseminating knowledge acquired e.g. at EU level training, a lack of training in data protection and the fact that not all Member States offer comprehensive training for the 24/7 officers.

The training offer for field officers not as well developed as that for SPOC officers. There are some possibilities, such as staff exchanges and courses at MEPA, but these are only available to a limited number of field officers. As some Member States are contemplating SIENA roll-out at field level, there is a need for training on SIENA in the field.

4.3.1.3 Recommendations

In general, it is recommended that strategies be developed at EU and national level that define knowledge needs and training gaps as well as concrete plans on how to cater for these needs. There is a need to make full use of the existing training offers and for the offers to be enhanced where necessary. To achieve this, the Member States, the Commission, CEPOL and Europol need to contribute and work together.

- Training should not be ad hoc; the types of competencies necessary and the way these can be taught needs to be defined. It is considered as highly relevant that future efforts on training be based on learning strategies developed at EU and national level, which are based on an examination of the training needs. The following points should be taken into account:
  - Strategies should take into account the LETS Communication (cf. the specific action point below), but adapted in accordance with national structures;
  - These strategies should take into account that practically oriented training is considered most useful;
  - E-learning should be considered as a complementary means of providing training to many participants at low cost;
  - The existing action plan in the LETS, which provides relevant actions relating to training on law enforcement information exchange, should be pursued further while taking into account CEPOL's budgetary situation; and
  - Funding provided by the ISF should be exploited to realise the learning strategies.
- EU training should be as beneficial as possible. In particular, it is considered important to encourage staff returning from EU positions and training (Europol, Interpol) be systematically used as multipliers for disseminating expertise/knowledge to relevant colleagues. For this purpose, the relevant departments could consider regular or ad hoc meetings to exchange any new lessons learnt.
- In general terms, it is considered relevant that the following topics be included in the EU level offer of training for law enforcement officers:
  - European rules on data protection: these should be taken up to greater extent to promote a common level of knowledge and understanding of the role of data protection in everyday police work.

- Training on SIENA: this should be included in CEPOL's offer, e.g. in the form of a webinar. This should be supported by Europol that is already active in raising awareness about SIENA.

- Specific actions are considered relevant with a view to ensuring that **field officers** are aware of the possibilities for exchanging information and the national institutions in place:

  - Up-to-date information the SPOC, including when it should be contacted, should be accessible on the intranet. SPOC roadshows should be considered to inform field officers about the benefits and modalities of information exchange as well as the workings of the SPOC. Such sessions should include the possibility for field officers working on practical case examples, as this is seen as being most effective in raising interest.

  - Topical training on relevant crime areas (e.g. drugs or THB) should include information about information exchange.

  - It would be useful to develop a package for a training course about "International police cooperation and information exchange within the EU area" targeted at field officers. This package should include training materials and instructions, which could be used in the Member States. It would then need to be ensured that the materials are translated and used. The possibilities for funding this should be explored.

- Specific actions are considered relevant with a view to ensuring that **SPOC staff** receives adequate training and support:

  - An introductory training session about the set-up of the SPOC and the relevant legal instruments and procedures should be available to newcomers. Such training should complement existing mentoring programmes.

  - Staff exchanges for SPOC staff to other Member States and to Europol need to be further promoted, in particular by securing sufficient resources for such programmes. It would be useful to raise awareness among managers in law enforcement positions about the benefits of such programmes. This could be done, for example, in the context of international conferences. In this context, good use should be made of the funding opportunities available at the EU level.

  - It needs to be ensured that SPOC officers have sufficient language skills by integrating language training in the training programmes for SPOC officers.

  - Consideration should be given to developing a specific training package that covers all channels and instruments that are relevant for information exchange. The current ambiguities in relation to the SFD should be taken into account in this context. As part of this package, a manual building on the manual developed under the IMS (Information Management Strategy) action list should be offered. This should stipulate in a consistent manner the procedures to be used for international information exchange. Consideration should be given to integrating the guidelines on the choice of channel into this manual.

4.3.2 Further general considerations

In addition to the topics covered above, our study aimed to point to the main remaining gaps to efficient and swift cross-border information exchange. These relate to horizontal challenges that apply to all of the topics discussed above. The challenges identified are discussed under the following headings:

- Policy aspects;
- Lack of consistency and need for governance;
- Cross-cutting factors hindering the application of existing instruments;
- Instruments/channels/tools gaps in current tools/need for additional tools; and
- Privacy and data protection.

4.3.2.1 Policy aspects

Based on the input received during this study, it seems that there is **room for further developing EIXM**. While the conclusions of the EIXM Communication (in particular the fact that no new instruments other than consolidation are needed), were appreciated by the stakeholders consulted, some believed that the Communication did not go far enough. In particular, some interviewees indicated that EIXM does not give sufficient guidelines to Member States. The EIXM model is seen as focusing simply on stocktaking and not so much on streamlining and harmonising instruments. An overall vision, which would help in defining future actions, is deemed to be still lacking.

Closely related to this point is the fact that the different EU policy documents (IMS, EIXM and others) seem to lack a common and wider context, and there is no roadmap with milestones set out for different objective to be reached. Strategies, policies and instruments are to a large extent divided per instrument, which hampers cross-domain usage, coordination and harmonisation.

It should be highlighted here that the end of the transitional period on 1 December 2014 completed 'supranationalisation' of the former third pillar and a greater role for EU institutions, including the Commission and the Court of Justice. Therefore a greater focus on the implementation of third pillar law by Member States is to be expected.

'Lisbonisation' of the third pillar *acquis* is being accompanied by the introduction of new proposals amending existing legislation (see draft Europol Regulation[213]). The impact of such law reform on EIXM remains to be seen. There is a need to examine the relationship of existing instruments with post-Lisbon initiatives in the field of judicial co-operation (such as the proposal for a Regulation establishing the European Public Prosecutor's Office[214] or the Directive on the European Investigation Order in criminal matters[215]) as well as initiatives enabling public-private partnerships in the field of surveillance (e.g. proposals for the establishment of an EU PNR system[216]).

---

[213] COM (2013) 173 final (http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2013)0173_/com_com(2013)0173_en.pdf).

[214] COM (2013) 534 final (http://eur-lex.europa.eu/legal-content/en/ALL/;ELX_SESSIONID=GlHMJsYGkrXj7288hwfr9pKDmsvh4vvpGb9v1ntG2nF14LvxC14c!-1821012834?uri=CELEX:52013PC0534)

[215] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, c.f. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN. The transposition deadline of the Directive is 22 May 2017.

[216] For further information see: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/passenger-name-record/index_en.htm.

4.3.2.2 Lack of consistency and need for governance

The EIXM Communication's focus on consolidating the current information exchange landscape is still appropriate on the basis of the findings of this study. This was supported by many of the stakeholders consulted who argued that there are numerous options for exchanging information, but that these are not always implemented and used correctly and consistently. This is due to several reasons, which are discussed below.

Clear rules on data capture, quality control and agreements on the legal basis used when capturing and using the data, common procedures, etc. are not in place for all aspects of cross-border information exchange. Indeed, several stakeholders indicated that there are many systems and channels at EU level and the guidelines on using them are not always clear. SIS and SIRENE were mentioned as good examples of detailed rules existing.

There was a perception among interviewees that there is **little guidance and cooperation** at present on law enforcement information exchange and the governance of instruments and tools is spread over several fora. At the same time, many noted the good experiences with cooperation in the SIRENE Working Group of the Council. It was also regretted by some policy makers that the role of Europol and eu-LISA has currently not been considered to a sufficient extent. It was argued that these agencies would be well placed to play a bigger role in governance of some of the measures covered in EIXM.

Several interviewees and participants in the expert panel argued that the relevant organisational set-up as well as the use of the different instruments and tools are not sufficiently streamlined and believed **that the absence of more binding EU level rules hinder effective information exchange**. On the other hand, there is a certain level of reluctance among certain groups of stakeholders when specific measures for harmonisation are proposed (such as standardising the choice of channels, training requirements or defining concrete criteria for SPOCs).

4.3.2.3 Cross-cutting factors hindering the application of existing instruments

A number of challenges have been identified that hamper the use of the instruments.

First, the instruments and tools considered are **not fully implemented in all of the Member States**. Therefore, it has not been possible to realise their full potential.

Political will has to be the basis for any progress in the implementation and use of the different instruments. Some interviewees regretted that this is sometimes lacking, in particular in relation to the implementation of Prüm. There is significant support and funding offered at EU level, which it was believed has not been sufficiently utilised. Some interviewees also felt that the issue of international police cooperation is often not regarded as a priority compared to resource considerations for national law enforcement authorities.

Shortcomings relating to human resources, financing and IT infrastructures are general challenges that may hinder implementation in the Member States. A very important aspect to take into account is the fact that the **volume of information exchange has been increasing**[217] by some fivefold over the past few years. However, the resources, and in particular the staff available, have not increased. Thus, it is highly important that information exchange become increasingly efficient.

[217] "All Member States note an increase, with an average of 10% to 20% per year, in the incoming requests during the past ten years." *Answers to the Questionnaire on action 2 of IMS Action List No 3*, Council document, DS 1800/13, 2 October 2013.

In addition to knowledge about the existing instruments and tools for information exchange, **language knowledge**[218] is still an area where there is room for improvement. We observe that SPOC officers do not always speak a second language fluently. Furthermore, it was regretted that not all SPOC officers have a sufficient knowledge of English[219], which is actually the most common language of communication[220]. As mentioned in section 4.3.1.1, the language training offer currently does not seem sufficient.

The **differences in the legal and administrative systems** of the Member States and in data protection legislation can be considered as further obstacles.[221] However, taking these differences into consideration, the progress made in the past few years is very positive.

Mutual trust is one of the most important factors in cross-border information exchange. While Member States generally appear to trust each other[222], some resistance to share information has been reported by interviewees in our study. A few of our interviewees indicated that some police officers do not feel comfortable with sharing data with other Member States, or with Europol, as they might feel that this means that they will be letting the investigation out of their hands. Fear of leaks in case information is transmitted is also a concern.

Finally, **technical differences** hamper interoperability.[223] Functional interoperability can be reached by using agreed definitions of the data exchanged. Technical differences (e.g. formats, messaging standards, message exchange technologies) can hamper interoperability since these impact on reliability, availability and secure transfer, and this also has an impact on the ease with which changes can be implemented.

4.3.2.4 Gaps regarding the current instruments, channels and tools

In general, the majority of stakeholders consulted indicated that there is currently no need for new tools, but rather for consolidation (cf. section 4.3.2.2). Yet a couple of gaps were identified relating to the current landscape of tools and channels. Some stakeholders pointed to gaps relating to existing tools or channels and some identified the need to introduce additional measures.

In order to fully exploit existing instruments and for any further extension in the area of police information exchange, stakeholders expressed a need for **practical and useful tools** (e.g. common software solutions, formats, systems) that support the legal instruments. An example of the need for this is the ambivalent situation relating to the SFD. Member States use e-mail, the SFD forms, SIENA or any other format/tool available at national level to manage requests. There is no common approach. For SFD requests, there is a function in SIENA that could fulfil these needs, but SIENA is currently not used to a substantial extent by all Member States.

---

[218] See also *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments,* ICMPD (2010), pp. 83 ff.
[219] See also the LETS Communication, COM(2013) 172 final, p. 5 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0172:FIN:EN:PDF).
[220] According to some interviewees, information exchange among countries that can understand the same languages (e.g. German speaking countries, French speaking countries, Slavic countries) is easier and thus might be more frequent.
[221] These factors were mentioned e.g. in our web-based survey as well as in the *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD (2010), p. 8.
[222] This was also the finding of *ICMPD (2010): "The Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments", pp. 83 ff.*
[223] *Study on the Status of Information Exchange Amongst Law Enforcement Authorities in the Context of Existing EU Instruments*, ICMPD (2010), p. 8.

The need for **multi-query functions**[224] in the area of police information exchange was mentioned by many interviewees and by expert panel participants. An information exchange platform, such as that discussed in section 4.2.2.4, could potentially fulfil these needs. ADEP is a somewhat similar idea but focuses mainly on information that is currently not exchanged. The idea of a common query function is also mentioned in a confidential European Commission mapping paper: "Member States voice the opinion that a missing link in the information exchange legal architecture is the very knowledge if a piece of information sought is at all available and if so, in what Member State. In that context most participants expressed their strong support for a tool, which would fill this gap by a kind of index for police Law-enforcement information and intelligence." This need could partly be addressed by the planned follow-up project to UMF II on interoperability, using ideas from the IXP concept and the UMF standard.

Furthermore, **user friendliness and language support** are vital for creating any tool and to make good use of the existing tools. Users appreciate automated translation and tools integrated in national systems. Interviewees believe there is at present too much downloading and manual work at Europol and in Member States.

4.3.2.5 Privacy and data protection

As noted above, the Treaty of Lisbon has brought some changes that have an impact on the implementation of EIXM. With regard to privacy and data protection, the integration of the EU Charter of Fundamental Rights into the Treaty Framework will have effects on EIXM. The CJEU has already confirmed the broad scope of applicability of the Charter[225]. Articles 7 and 8 of the Charter (on privacy and data protection) are of particular relevance in this context.

From a broader privacy perspective, it is imperative to examine any information exchange under EIXM not only from a data protection perspective, but also from a broader privacy perspective. Constitutional Courts in Member States, the European Court of Human Rights and the Court of Justice of the European Union have all delivered seminal rulings on the limits which human rights place on surveillance and the content of databases.

Different rulings by the European Court of Human Rights (e.g. Marper[226], Brunet[227]) are of relevance. In these cases, the Strasbourg Court found breaches of Article 8 via the retention of personal data (including DNA) of individuals not convicted of a criminal offence. In both cases the Court stressed the lack of proportionality and the risk of stigmatisation of affected individuals. These cases raise fundamental questions about the use of technology and its limits. In addition, national constitutional courts' rulings on data retention (including in Bulgaria, Germany, and Romania) need to be considered. The Courts annulled national implementation of the Data Retention Directive[228] and linked the privacy challenges with challenges to citizenship and the rule of law in the relationship between the individuals affected and the state.

[224] A function that allows for searching different databases at once, e.g. using indexes.
[225] C.f. the Fransson case.
[226] Case of S. and Marper v. the United Kingdom http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-90051.
[227] Case of Brunet v. France http://hudoc.echr.coe.int/sites/eng/pages/search.aspx.
[228] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

Nevertheless, data protection and information exchange do not need to be regarded as opposites. The relevant opinions of the EDPS[229] do not raise major concerns. While the EDPS insists on safeguarding traditional data protection principles, information exchange is not considered controversial as such.

As far as the day-to-day application of data protection principles are concerned, we note that access rights need to be properly managed and the purpose limitation principle adhered to. Even if digital access rights are respected, the oral transmission of data to an inappropriate person is a possibility in the workspace of the SPOC. It is worth noting in this regard that the Data Protection Reform Package[230] also proposes the presence of data protection officers in SPOCs.

4.3.2.6 Conclusions

The conclusions of the EIXM Communication (in particular the fact that no new instruments are needed but only consolidation), are appreciated by the stakeholders consulted. However, the EIXM model focused on stocktaking, and an overall vision in the area of information exchange is not provided.

Differences in national legal and administrative systems are general obstacles to achieving better information exchange. However, taking these differences into consideration, the progress made in the past few years is very positive.

There seems to be a need for more EU level overall governance and guidance in the area of police information exchange. The increased competences of the Commission under the Lisbon Treaty are an opportunity.

Progress on and a common understanding of the SPOC concept and the choice of channel are hindered by the lack of binding rules.

Even though there is funding and support at EU level, there seems to be a lack of political prioritisation that in some cases hinders the implementation of EU instruments.

The delays in the implementation of Prüm and the difficulties in the application of the SFD create a situation in which progress is further slowed. These factors seem to decrease the motivation in some Member States to put effort into the implementation and application of EU instruments if they see that their counterparts are not doing the same.

Information exchange has increased but the allocation of resources in Member States working in the area of information exchange has not followed this increase.

There is a lack of awareness among police corps on the availability and potential of information exchange, which also is related to existing training programmes not meeting relevant needs fully.

---

[229] See Opinion of the European Data Protection Supervisor on the EIXM Communication (https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-04-29_EIXM_EN.pdf).

[230] C.f. http://ec.europa.eu/justice/data-protection/.

4.3.2.7 Recommendations

Based on the findings of this study, we recommend, in the mid-term, developing the European Information Exchange Model further with a broader look at information exchange, involving all relevant institutions (including e.g. the Committee on Internal Security (COSI), OLAF, Interpol), as well as related policy areas such as border management and customs. The following aspects should be considered in this context:

- Substantial emphasis should be placed on the implications for privacy and data protection and an assessment of the current compliance of EIXM with data protection should be carried out as a basis for this;
- EIXM should also involve a roadmap element, which should define clear goals, set a clear timeframe for these goals, and agree on measures/activities and milestones to reach the goals;

There are certain pre-conditions for the successful implementation of EIXM (in its current state or in a broader sense):

- Legislative measures adopted under the post-Lisbon legal basis, providing binding rules to remove the ambiguities highlighted in this report, are considered important; and
- It is necessary that appropriate resources are allocated to SPOCs, responding to the growth in volume of information exchange requests.

In the continued work to improve and harmonise information exchange within the law enforcement area, the new Schengen evaluation mechanism would be a very useful tool. The findings resulting from the SEM could make substantial contributions to the future of the EIXM. The more prominent role of the Commission in the SEM, as well as the increased competences through the Lisbon treaty, could facilitate the development of further policy guidance, or even legislative measures, in the field of law enforcement information exchange.

Indeed, SIS II and SIRENE, with their long history and a high degree of success in operational use, provide a number of lessons learned that could be looked at for use in other areas as well. Examples of elements related to the SIS II and SIRENE that could be considered in other areas are:

- In the event of Prüm hits, SPOCs could learn from common instructions for the SIRENE offices in case of SIS II hits, regarding what action to take in processing any further information exchange needed;
- UMF can be used in order to reduce free texts which in the SIS/SIRENE context are avoided and replaced by codes, representing exactly the same content in all countries;
- SIENA could be regulated as default channel for exchanges within the scope of the SFD as the SIS II channel is regulated for supplementary SIS II information;
- Regularly organised meetings for following up the use and the efficiency of SIS II and SIRENE, where enhancements and developments are discussed, involving representatives of the users could be taken as a good example; and
- A manual should be prepared with best practices which is also used in evaluations such as the SIRENE manual.

Annexes

Annex 1: Analytical Framework

Research questions	Judgement criteria	Indicators/data	Sources of information
What is the impact of the transposition and application of the Swedish Framework Decision (SFD) in daily practice?	**Awareness** of the SFD among responsible officers in the field	- Knowledge of the SFD, and its main principles - Knowledge of the national legislation implementing it (including definitions, concepts and procedures) - The extent to which officers working with these procedures feel that they are an important part of their daily work	Fieldwork interviews Telephone interviews (Visit to Europol) (Preliminary interviews)
	Compliance with the SFD's legal requirements in daily practice, and its **impact** (in particular regarding Art 3 (3) and (4) and Art 6 (2), where relevant)	- The perception of officers working with SFD procedures on the extent to which the SFD has an impact - Statistics on the number of forms sent and received - Experiences with the application of the principle of equivalent access (including via a judicial authority) - Statistics on the application of the principle of equivalent access (including via a judicial authority) - Experiences and national instructions/practice concerning the modalities of sharing information or intelligence with Europol - Europol statistics on the number of cases where Member States shared information or intelligence with Europol	Web-based survey Preliminary interviews Telephone interviews Fieldwork interviews Desk research (on national statistics made available to the study team) Visit to Europol

Research questions	Judgement criteria	Indicators/data	Sources of information
		- National practices regarding sharing information or intelligence with Europol (including whether further possibilities to share information exist and are desirable)	
	The amount of SFD requests to which the requested authority **refused to reply**	- Statistics on the number of cases where the requested authority refused to reply to a SFD request - Qualitative data regarding the extent to which requests are refused Qualitative data concerning the reasons why requests are refused in practice	Fieldwork interviews Phone interviews Desk research (on national statistics made available to the study team)
	The **reasons** why SFD may not have improved the data exchange as expected (and **possibilities to overcome** the alleged lack of impact)	- Qualitative data regarding the reasons why the use of SFD remains limited - Perceptions of ▪ (both operational and strategic level) officers working with SFD procedures; ▪ DG HOME experts; ▪ Europol experts; ▪ EU stakeholders.	Desk research Web-based survey Preliminary interviews Phone interviews Fieldwork interviews Visit to Europol Expert panel
How are the requests after the Prüm hits followed-up by the competent authorities in the countries? **What are the links with the SFD?**	Specific **mechanisms for Prüm follow-up** requests after a "Prüm hit" and links to SFD	- National procedures in place for following up requests ▪ Subject of the requests ▪ Specific procedures in place ▪ Time for answering the requests ▪ Obstacles and constraints ▪ Links with SFD	Phone interviews Fieldwork interviews Web-based survey Desk research (based on information received during interviews)

Research questions	Judgement criteria	Indicators/data	Sources of information
	Gathering statistics about Prüm **'hits' that were actually followed up** in investigations (most relevant for DNA data)	- Statistics on the number of post-hit SFD requests	
What are the national approaches toward the choice of channel?	**National approaches**, including defined criteria for choosing a channel or related plans for the future	- Existence of national instructions for choice of channel and their content - National practices regarding the use of SIENA as a channel - Qualitative data concerning the legitimate reasons police officers see for using a channel other than what is foreseen by EU law - National preference for (and experiences with) channel for police cooperation exchanges previously using SISNET	Desk research (based on information received during interviews) Web-based survey Phone interviews Fieldwork interviews Visit to Europol Expert panel
	Main **barriers** that impede standardisation on national level and possible ways of how to overcome them	- Experience of interviewees working with exchange of information regarding the application of national instructions/practices on the choice of channel, perceptions of possible barriers to standardisation	
	Aspects preventing police from using **Europol channel/SIENA**, or concrete requirements which would increase its suitability for police-to-police contacts	- Experiences of interviewees working with exchange of information regarding using Europol/SIENA, possible difficulties of use - Qualitative data regarding the technical abilities in Member States to use SIENA - Qualitative data regarding the level of access of SIENA for police officers - Qualitative data regarding the availability of national training courses on using SIENA	

Research questions	Judgement criteria	Indicators/data	Sources of information
How is the concept of Single Point of Contact applied?	**Concepts** of Single Points of Contact (SPOCs) in Member States and to what extent they reflect the features suggested in EIXM **Obstacles** to establishing comprehensive SPOCs and possible ways of how to overcome them **Limits to the SPOCs concept** as well as possible alternative organisational solutions to achieve more effective information exchange	- The nature of international police cooperation departments in Member States - Nature and number of channels brought together in the SPOCs - Perception of interviewees of the potential difficulties of establishing a SPOC - Perception of interviewees regarding the limitations of the SPOC concept and its added value in operational work - Opinion of interviewees regarding different ways to achieve more efficient information exchange - Quantitative data concerning the operational limitations of SPOCs - Qualitative data on systemic reasons for the limitations of the SPOC concept	Desk research (based on information received during interviews) Web-based survey Phone interviews Fieldwork interviews Visit to Europol Expert panel
What could be the technical development beyond UMF II that could help achieving the objectives of EIXM?	Technical developments which could help achieving the objectives of EIXM and serve as basis for advancing information exchange (such as automation or improving technical interoperability and possible related ongoing efforts)	- Quantitative (and, where available, qualitative) data regarding ▪ awareness of the fundamental features of UMF II ▪ plans of Member State administrations to implement UMF II in their national systems ▪ any gaps in the current format	Desk research Web-based survey Phone interviews Expert panel
What are and what could be the training measures supporting cross-border information exchange?	Assessment of training measures which support cross-border information exchange and the implementation of EIXM recommendations	- Number of national trainings provided on cross-border information exchange - Nature and general content of national trainings provided on cross-border information exchange - Perception of added value of these trainings by attendees	Desk research Web-based survey Phone interviews Fieldwork interviews

Research questions	Judgement criteria	Indicators/data	Sources of information
		- Number, duration and purpose of exchanges of SPOC staff - Opinions of stakeholders on possible improvements	
What are the main remaining gaps to efficient and swift cross-border information exchange?	Assessment of main remaining gaps to efficient (i.e. value for the resource involved) and swift cross-border information exchange	- Perceptions of the gaps by the different stakeholders involved; - Identification of the most recurrent gaps; - Classification of the gaps according to their domains, e.g. technological, organizational, legal, cultural.	Desk research Preliminary interviews Phone interviews Fieldwork interviews Visit to Europol Expert panel
To what extent are existing national instruments used to exchange data from national police records?	(In particular) the **possible overlap** between national databases used for uploading data to the Europol Information System (EIS) with databases which a Member State would use for feeding a dedicated European Police Records Index System (EPRIS)	- Check and clarification on how the existing definition is understood by the concerned stakeholders in the MS, e.g. understanding of the definition of "a Police record" that leads to an EPRIS. - The nature and content of national databases used for uploading data to EIS - The nature and content of databases Member State would use for feeding EPRIS - Opinion of police officers regarding the possible structural advantage of EPRIS compared to EIS	Desk research Web-based survey Preliminary interviews Fieldwork interviews Phone interviews Visit to Europol Expert panel

Annex 2: Interview guides

The interview guides presented below follow the same breakdown as the proposed routing of the web-based survey (field officers and their hierarchy at law enforcement authorities, SPOC staff and policy makers).

The interviews were conducted in such a way that the role of the concerned organisation and the interviewed person was taken into account.

The questions also took into account and referred back to, whenever relevant, the outcome of the web-based survey. The aim of this document was thus to serve as a guide from which the interviewers were able to pick relevant questions by taking into account what they know already (based on the survey results) and what issues should be further investigated.

For all questions wherever appropriate, interviewees were prompted to give specific recommendations for the way forward.

Background information

Interviewee name	
Institution and position	
Interview date and place	

Introduction

- *Description and timeline of the project;*
- *Purpose of the semi-structured interview;*
- *Request for any national statistics they can provide us with concerning their practices of exchanging information.*

1. Please briefly describe your position and your role in relation to international cooperation among law enforcement officials, and communication channels used for information exchange.

Interview Guide A – Field officers and their hierarchy at law enforcement authorities

Impact of the Swedish Framework Decision

1. Are you aware of the possibility under EU law to exchange police information between EU Member States' police officers?

2. In case you were confronted with a case where you have reasonable grounds to believe that another EU Member State's police have information that could help you, what would you do? In case you already had similar cases, please provide a concrete example of a case, the actions taken by you and the reasons for this.

3. Do you have any national/regional instructions/manual you can turn to for guidance on what actions to take in similar cases? How do you make sure in practice that foreign requests are treated equally as domestic requests?

4. What type of data in such cases (if any) do you think should be shared with Europol?

Choice of channel and Prüm follow-up procedures

5. Do you think it is possible for your police officers to check whether another EU Member States' database contains information on a fingerprint, DNA data or vehicle registration data you are interested in?

6. If you are aware of the so-called Prüm procedure, what procedure do you follow if you received a hit? Do you see a problem with this procedure? If yes, where?

7. On what basis do you decide which channel you will use? If you do not use SIENA, why?

8. Is your SPOC involved in the follow-up of Prüm hits? If not, why?

The concept of SPOC

9. Do you have a Single Point of Contact[231] in your Member State? In what cases do you turn to them?

10. Are you satisfied with their response time and availability?

11. What benefits do you see in having a SPOC?

12. Are there limits to the usefulness of a SPOC and what such limits/constraints do you see? How could these be addressed?

13. Do you see alternatives to the SPOC concept which could help achieve a more efficient information exchange?

Training

14. Have you received any training about information exchange in the context of cross-border law enforcement cooperation (at the academy, at national/regional or at EU level)? What subjects were covered in these and how useful did you find them for your work?

15. What additional training in this area would you need to be better able to cope with related tasks?

[231] A Single Point of Contact (SPOC) is a 'one-stop shop' for international police cooperation.

Other issues

16. Where would you see that there are gaps and needs for improvement concerning the current way information exchange is carried out among Member States? (Do they relate to technology, law, organisation, funding, staff, etc.?)

17. In case you call directly a colleague from another Member State to request information informally, do you include a formal request afterwards in one of the communication channels? In your opinion, how big of a share of all the requests you are aware of go through informal channels?

18. In what way do you share data with Europol?

Interview Guide B – SPOC staff

Impact of the Swedish Framework Decision

1. How is it ensured that field officers are aware of the relevant procedures they can/should use? Are there national/regional instructions/manuals in place?

2. Is the use of SFD an important part of your work, explicitly or implicitly? Have you encountered any particular problems with the relevant procedures (besides the forms)?

3. Do you consider it mandatory to comply with the provisions of the SFD when you receive a request?

4. Is the principle of equivalent access[232] working satisfactory in your exchange of information with other Member States? Have you refused requests or saw your requests be refused by other Member States? Based on what grounds? How do you make sure you do not discriminate foreign requests (equivalent treatment principle)?

5. Are you regularly sharing data with Europol, as requested by the SFD, and if so, in which cases? Do you have statistics on this?

6. What would be the nature and extent of the problem if you did not receive information under the SFD?

7. Could you give examples of an actual or typical cases of information exchange with another Member State?

Choice of channel and Prüm follow-up procedures

8. What instructions are used when choosing a channel, and do these instructions have specific procedures or rules for the use of SIENA? Are they sufficiently detailed?

19. Is your SPOC involved in the follow-up of Prüm hits? If not, why?

9. In what circumstances do you see it necessary to choose an alternative channel than what is foreseen in EU law and/or in national/regional instructions? What are the reasons for this?

[232] The principle of equivalent access obliges Member States to process and answer queries from other Member States' law enforcement authorities the same way as they handle requests by national bodies.

10. What are your Member States' experiences with SIENA? If it is not used (at all or to the extent recommended), what are the reasons for this?

11. Do you have proposals for enhancements or see problems that need to be solved, which could change the current use of channels – in order to better enable information exchange?

12. Do you have any plans in the pipeline for the future?

The concept of SPOC

13. Can you describe how your SPOC is organised (including, if possible, their budget, FTEs and list of tasks)?

14. Does your SPOC have the following features?

    - ✓ SPOC guidelines including national/regional rules for the choice of channels
    - ✓ Integrated national case management and workflow system supporting all channels (SIENA/ Europol, SIRENE, Interpol) and using the UMF II data model
    - ✓ Validating requests in a consistent way, systematic quality checks
    - ✓ SPOC staff is specifically trained
    - ✓ Availability of representatives of all relevant law enforcement authorities, like customs, border police and where possible judicial authorities
    - ✓ SPOC available 24/7
    - ✓ SPOC has direct access to relevant national/regional databases

15. Are there any additional features you consider relevant?

16. What is your experience concerning communication with other SPOCs? Have you had any cases where the ability of the requested Member State was hampered by their national/regional procedures? Have you discovered any misunderstandings between national ways of working? Would you have suggestions as to how to improve communication among SPOCs?

17. What benefits do you see in having a SPOC? What do you think are the potential difficulties of establishing a SPOC?

18. Are there limits to the usefulness of a SPOC and what such limits/constraints do you see? How could these be addressed?

19. Do you see an alternatives to the SPOC concept which could help achieve a more efficient information exchange?

20. Can a SPOC offer added value in terms of data protection compliance?

Prospects of technical developments beyond UMF II

20. Are you familiar with the specification of UMF II?[233] Do you think these will be implemented in your Member State? Do you think the specifications and tools (forms) would cover your needs, or are there gaps?

[233] Universal Message Format (acronym: UMF) refers to the common framework for the structured, cross-border information exchange between law enforcement authorities and/or organisations. UMF defines a common vocabulary and logical structures for commonly exchanged information (e.g. persons, offences, etc.).

Training

21. Have you received any training about information exchange under cross-border law enforcement cooperation (at the academy, at national/regional or at EU level)?

22. Have you participated in an exchange of staff with other Member State, and if yes, what were your experiences?

23. In case you have not participated in such a training or exchange of staff, what would you expect from such training? Who/which stakeholders would be best placed to conduct such training?

21. In case you have participated in such a training or exchange of staff, what subjects were covered in these and how useful did you find them for your work? What was missing in the training?

Exchange of police records

22. Do you see a need for automatic access to national police records in other countries or to replace current manual procedures by more enhanced automated procedures?

23. Is there a clear definition in your country of 'police records'?

24. In relation to proposals for extended and automated exchange of police records (EPRIS, ADEP), what do you think their structural advantage would be compared to feeding the Europol Information System?

24. What type of national/regional databases do you think could be used to feed a potential future EPRIS/ADEP? Do these differ from the ones used for EIS?

Remaining gaps to efficient and swift cross-border information exchange

25. Where would you see that there are gaps and needs for improvement concerning the current way information exchange is carried out among Member States? (Do they relate to technology, law, organisation, funding, staff, etc.?)

26. In your experience, are there times when data is transferred, without this data being understandable for the receiver?

Interview Guide C – Policy makers/ Central police senior officers

Impact of the Swedish Framework Decision

1. How is the SFD implemented in your national/regional legislation and how is it ensured that field officers are aware of the relevant procedures they can/should use? Are there national instructions/manuals in place?

2. Do you think the principle of equivalent access is working satisfactory in your exchange of information with other Member States? How do you think efficiency can be measured, beyond looking at the evolution of number of requests?

3. Are your authorities regularly sharing data with Europol, as requested by the SFD, and if so, in which cases? Do you have statistics on this?

4. Have your Member State refused a request by another to exchange information? Have your request been refused? What were the grounds for these refusals?

5. What would be the extent of the problem if you did not receive information under the SFD?

6. To what extent do you think information obtained via SFD exchange is used in a court case?

Choice of channel and Prüm follow-up procedures

7. What are your national Prüm follow-up procedures?

27. Is your SPOC involved in the follow-up of Prüm hits? If not, why?

8. Do you have national/regional instructions in place for choosing a channel, and if yes do these instructions have specific procedures or rules for the use of SIENA?

9. In what circumstances do you see it necessary to choose an alternative channel than what is foreseen by EU law and/or in national instructions?

10. What are your Member States' experiences with SIENA? If it is not used (at all or to the extent recommended), what are the reasons for this?

11. Do you have proposals for enhancements or see problems that need to be solved, which could change the current use of channels – in order to better follow the EIXM recommendations?

The concept of SPOC

12. Do you have SPOC in your Member State? Can you describe how it is organised?

13. Does it have the following features?

    - ✓ SPOC guidelines including national/regional rules for the choice of channels
    - ✓ Integrated national case management and workflow system supporting all channels (SIENA/ Europol, SIRENE, Interpol) and using the UMF II data model
    - ✓ Validating requests in a consistent way, systematic quality checks
    - ✓ SPOC staff is specifically trained
    - ✓ Availability of representatives of all relevant law enforcement authorities, like customs, border police and where possible judicial authorities
    - ✓ SPOC available 24/7
    - ✓ SPOC has direct access to relevant national databases

14. Are there any additional features you consider relevant?

15. What kind of obstacles (if any) have you met, or are still facing in setting up a SPOC that has these features?

16. What benefits do you see in having a SPOC?

17. Are there limits to the usefulness of a SPOC and what such limits/constraints do you see? How could these be addressed?

18. Do you see alternatives to the SPOC concept which could help achieve a more efficient information exchange?

19. Can SPOC offer added value in terms of data protection compliance?

Prospects of technical developments beyond UMF II

20. Are you familiar with the specification of UMF II?[234] Do you have plans for implementing UMF II in your Member State? If yes, do you foresee or have found problems to carry out this implementation?

21. Do you find the UMF II specifications and tools (forms) cover your needs, or do you see any gaps?

Training

22. Does your staff participate in regular training (provided nationally or at EU level) on information exchange? If yes, what topics are covered (e.g. specific to Prüm, to SFD, or other approaches)? Is such training also part of the regular police academy curricula in your Member State?

23. Are you exchanging staff with other Member States and if so, to what extent?

24. What is your view of the added value of the existing training and what improvements would you like to see?

Exchange of police records

25. Do you see a need for automatic access to national police records in other countries or to replace current manual procedures by more enhanced automated procedures?

26. Is there a clear definition in your country of 'police records'?

27. In relation to proposals for extended and automated exchange of police records (EPRIS, ADEP), what do you think their structural advantage would be compared to feeding the Europol Information System?

28. Do you think it would be possible to set up national indexes and give other Member States direct access?

29. What type of national databases do you think could be used to feed a potential future EPRIS/ADEP?

Remaining gaps to efficient and swift cross-border information exchange

30. Where would you see that there are gaps and needs for improvement concerning the current way information exchange is carried out among Member States? (Do they relate to technology, law, organisation, funding, staff, etc.?)

[234] Universal Message Format (acronym: UMF) refers to the common framework for the structured, cross-border information exchange between law enforcement authorities and/or organisations. UMF defines a common vocabulary and logical structures for commonly exchanged information (e.g. persons, offences, etc.).

Annex 3: Glossary of terms

Abbreviation	Term	Explanation / Working Definition
ADEP	Automation of the Data Exchange Process	A project proposed by France, which seeks to enhance information exchange by facilitating automation of current manual procedures, such as the searching of national police databases.
AWF	Analysis Work File	While not within the scope of the present study, the AWF is an instrument used by Europol to store information related to ongoing operations in the Member States. AWFs include data on individuals and any other information that Europol National Units (ENUs; see below) may decide to add and allow Europol to provide operational analyses to support cross-border investigations.
CEPOL	European Police College	CEPOL is an EU agency established on the basis of Council Decision 2005/681/JHA. It plays a central role in providing training for senior police officers of the Member States on issues that are relevant to EU police cooperation. CEPOL functions as a network that brings together the national training institutes in the Member States.
	Channel of communication	This term can have various meanings and interpretations. For the purpose of this study, it refers to communication channels through which information and criminal intelligence are exchanged in the framework of EU police cooperation, including in particular: ➢ SIRENE Bureaux (see below); ➢ Europol National Units (ENUs; see below); and ➢ Interpol National Central Bureaux.
eCodex	e-Justice Communication via Online Data EXchange	eCodex is a project funded by the EU, which has as its aim to "improve the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability between legal authorities within the EU."[235] The participants are developing 'building blocks', i.e. tools in different areas ranging from safe transportation, to identity and document standard, to enable cross-border interoperability in the field of justice. To do this, eCodex is developing a container format and related metadata to facilitate cross-border exchange, as well as interpreting and processing of electronic documents.
ECRIS	European Criminal Records Information System	ECRIS provides an infrastructure for interconnecting registries of criminal records. In this context, Member States exchange information relating to convictions with one another using a standardised format.
EIF	European Interoperability Framework	This document contains a set of recommendations and guidelines for eGovernment services with a view to ensuring that public administrations, enterprises and citizens can interact across borders.
EIXM	European Information Exchange Model	Considering the complex and diverse landscape of instruments on information exchange in the field of police cooperation, the Commission was invited to assess the need for a European Information Exchange Model by the Stockholm Programme. The aim was to improve coherence and consolidation in streamlining information management and exchange. On this basis, the Commission presented its EIXM Communication (COM(2012) 735 final) in 2012, which contains recommendations on how to improve and streamline the use of existing instruments and tools created to facilitate information exchange in the law enforcement context.

[235] http://www.e-codex.eu/about-the-project.html

Abbreviation	Term	Explanation / Working Definition
EIS	Europol Information System	EIS is a database of information provided by Europol. It contains information on cross-border crime within Europol's mandate, the individuals involved and other related data. Information is mainly fed into the database by the Member States and Europol. The EIS serves as a reference system, which Europol uses for its analyses and Member States for investigations.
ENU	Europol National Unit	Europol National Units are national units designated by the Member States on the basis of the Europol Council Decision to fulfil the function of the only liaison body between Europol and the competent authorities of the Member States.
EPRIS	European Police Records Index System	In line with the Stockholm Programme, the Commission procured a study on the possible introduction of a European Police Records Index System (EPRIS). The idea was to enable police officers in one Member State to obtain information on whether a suspect is known to the police in another Member State. However, in the EIXM Communication the Commission concluded that such a new instrument is currently not needed.
eu-LISA	EU Agency for large-scale IT systems	eu-LISA started its operations on December 1, 2012. It is responsible for the operational management tasks for SIS II, VIS and EURODAC, ensuring that the systems function well and are kept running at all times. Its mandate may be extended to other large-scale systems in the future.
EURODAC	European Dactyloscopy database	EURODAC is an EU asylum fingerprint database established on the basis of Council Regulation (EC) No 2725/2000. A new version of this Regulation has recently been adopted (Regulation (EU) No 603/2013). While the EURODAC database could only be used for asylum purposes under the old framework, the new Regulation allows national police forces and Europol to compare fingerprints linked to criminal investigations with those contained in EURODAC.
Europol	European Police Office	Europol is an EU agency established on the basis of Council Decision 2009/371/JHA with the objective to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States. One of Europol's main tasks is to collect, store, process, analyse and exchange information. Europol has different databases and communication tools at its disposal, which Member States use to provide Europol with information and exchange information among them. In addition, Europol assists national authorities by providing specialist advice on investigations as well as strategic analyses.
	Europol Liaison officer	Europol liaison officers are law enforcement officers which are seconded to Europol by the Member States on the basis of the Europol Council Decision. They function as a contact point between Europol and the national authorities, representing the interest of the latter.
	Europol's Prüm helpdesk	The Prüm helpdesk was established at Europol in 2012 in order to support the Member States in relation to the implementation and application of the Prüm Council Decision. Support is offered in particular in the following areas: Technical support to implement the Prüm Decisions; support for States in their daily fingerprint and DNA information exchange mechanisms; and technical support with regard to further development of the network.
	I-24/7	Communication tool developed by Interpol, which may be used to exchange information with Interpol or on a bilateral basis. The system

Abbreviation	Term	Explanation / Working Definition
		enables authorised users to share sensitive and urgent police information and enables investigators to access Interpol's range of criminal databases.
IMS	Information Management Strategy	The IMS was developed by the Council in 2009. The aim of the strategy was to define how information should be stored and exchanged, as well as how the process should be managed. Thus, the document provides guidance on how to ensure an appropriate information exchange where supply of information takes account of both business needs and the rights of the individual in order to assist law enforcement authorities in how to efficiently organise an effective cross-border exchange of information.
	Interoperability	Interoperability refers to the ability of ICT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge. The Commission is working towards promoting interoperability to facilitate efficient cooperation and data exchange by public authorities across sectors and borders in the framework of the EIF (see above).
INTERPOL	International Criminal Police Organisation	Interpol is an international organisation with 190 member countries, which aims to facilitate international police cooperation by providing high-tech infrastructure and technical and operational support.
ISEC	Prevention of and Fight against Crime	Funding programme by the European Commission, which supports projects in the field of crime prevention and law enforcement. ISEC ran until 2013, and was succeeded by the Internal Security Fund (ISF; see below).
ISF	Internal Security Fund	The ISF is the European Commission's funding programme for projects related to internal security, established for the period 2014-2020. It will support the EU approach to law enforcement cooperation, including the management of the union's external borders. It will also cover the development of new IT systems, such as the future entry/exit system and the Registered Traveller Programme.
IXP	Information Exchange Platform	The Information Exchange Platform has been developed by Europol and presented to the DAPIX working group. The proposal includes developing a common portal with help functions, guidelines and also an operational multi-query function for all relevant EU systems.
MCT	Mobile Competence Team	The MCT was established in the framework of an ISEC funded project led by the German Federal Police, which ran from July 2011 until June 2013. Its aim was to support Member States in their technical implementation of the Prüm Decisions.
PCCC	Police and Customs Cooperation Centres	PCCCs were set up at internal frontiers on the basis of the Schengen Convention in order to address the "security deficits" in border regions. They are located at strategic positions and bring together, on one site, all the security authorities of all participating States.
	Personal data	Personal data is any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.
	Principle of availability	In 2005, the Hague Programme introduced the principle of availability, according to which information for law enforcement purposes needed by authorities of one Member State will be made available by the authorities of the Member State where the information is stored.

Abbreviation	Term	Explanation / Working Definition
	Principle of purpose limitation	A data protection principle, which states that data, as a basic principle, may only be used for the purpose of its original collection and processing.
	Prüm Decision	The term refers to Council Decision 2008/615/JHA, which provides for automated exchange of biometric data (DNA profiles and fingerprint data) and vehicle registration data for the prevention and investigation of criminal offences and maintaining public security.
SFD	Swedish Framework Decision	This refers to Council Framework Decision 2006/960 JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, which covers the exchange of information for the purpose of criminal investigations or criminal intelligence operations, with a particular focus on access to information. It introduces the concept of equivalent access, which obliges the Member States to process and answer queries from other Member States' law enforcement authorities the same way as they handle requests by national bodies.
SIENA	Secure Information Exchange Network Application	SIENA is a communication tool provided by Europol, which enables exchange of operational and strategic crime-related information and intelligence between Europol, the Member States and third parties that have cooperation agreements with Europol.
SIRENE	Supplementary Information Request at National Entry	A communication channel used for follow-up requests with regard to information stored in SIS II.
SIS II	Schengen Information System II	The Schengen Information System (SIS) was established as an intergovernmental initiative under the Schengen Convention. It is used by border guards as well as by police, customs, visa and judicial authorities throughout the Schengen Area and provides alerts on persons and objects. SIS II is the new version, which entered into force in 2013 and includes enhanced functions.
SLA	Service Level Agreements	A service level agreement is part of service contract, for example, between a governmental agency that uses an IT system and a firm that provides technical expertise to manage the system. In the agreement, the specific services are defined.
SPOC	Single Points of Contact	SPOC refers to a "one stop shop" unit for international police cooperation, with a multi-agency organisation within each Member State. The purpose of this institution is to make cross-border police cooperation more effective by subsuming competencies of different national offices or contact points.
s-TESTA/Testa NG	Trans European Services for Telematics between Administrations/ Testa new generation	A communication network of the European Union used for secure information exchange between the European public administrations. TestaNG is composed of various clouds, enabling several applications, such as SIS or EURODAC, to work under the Testa network.
UMF II	Universal Message Format 2	UMF II is fundamentally focusing on ensuring semantic interoperability because the use of common semantics across the participants of EIXM is of strategic importance for interoperability.