RES
PVBLICA
1995
ΑΘΗΝΑ

ICMPD
International Centre for
Migration Policy Development

JLS/2009/ISEC/PR/001-F3

Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments

December 2010

Reference of the contract
JLS/2009/ISEC/PR/001-F3

This study has been carried out for the Directorate-General Home Affairs in the European Commission as result of the procurement procedure **JLS/2009/ISEC/PR/001** for an amount of 144.896,35 €.

The report expresses the opinion of the International Centre for Migration Policy Development (ICMPD) who performed the study. These views have not been adopted or in any way approved by the European Commission and should not be relied upon as a statement of the European Commission's or the Home Affairs DG's views. The European Commission does not guarantee the accuracy of the information given in the study, nor does it accept responsibility for any use made thereof.

European Commission
DG Home Affairs, Directorate A
Rue du Luxembourg 46
B-1049 Brussels
HOME-PROCUREMENT-A4@ec.europa.eu

Reference of the contract

JLS/2009/ISEC/PR/001-F3

Project Team

Matjaz Saloven
Euan Grant
Peter Hanel
Viktor Makai
Kenneth Brent Hansen
Linas Belevicius
Angelika Pohnitzer

Acknowledgements

The Project Team expresses its appreciation towards many people across the European Union without whose co-operation and participation this Study Report could not have been drafted. Numerous representatives of law enforcement agencies were consulted and these have dedicated their time and effort for the benefits of this Study, providing replies to the questionnaires and sharing their opinions and insights.

Reference of the contract
JLS/2009/ISEC/PR/001-F3

International Centre for Migration Policy Development (ICMPD)
Gonzagagasse 1
A-1010 Vienna
Austria
www.icmpd.org

European Public Law Organization (EPLO)
16, Achaiou, Kolonaki
10675 Greece
www.eplo.eu

International Centre for Migration Policy Development and European Public Law Organization,
Austria and Greece, 2010

This publication has been produced with the assistance of the European Union. The content of this publication is the sole responsibility of ICMPD and EPLO and can in no way be taken to reflect the views of the European Union.

Table of Contents

Abbreviations and Acronyms

AFIS	Anti-Fraud Information System
AWF	EUROPOL's Analytical Work Files
CIS	Customs Information System
EAW	European Arrest Warrant
ECRIS	European Criminal Records Information System (under consideration)
EIS	EUROPOL Information System
EIO	European Investigation Order
ELO	European Liaison Officer (MS Liaison Officer at EUROPOL)
ENU	EUROPOL National Unit
EPRIS	European Police Records Index System (under consideration)
EU – PNR	Passenger Name Record
FADO	False and Authentic Documents Online (European Image Archiving System)
FIDE	Customs File Identification Database (EU database of MS' fraud cases for Custom's Authorities)
FIND	Fixed INTERPOL Network Database
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the MS of the EU
IPGS	INTERPOL General Secretariat
ISP	Internet Service Provider
IT	Information Technology
JIT	Joint Investigation Team
LEA	Law Enforcement Authority
LO	Liaison Officer(s)
MAA	Mutual Administrative Assistance
MAB	Mutual Assistance Broker system (successor to CIS and other AFIS systems)
MIND	Mutual INTERPOL Network Database
MLA	Mutual Legal Assistance
MoF	Ministry of Finance
MoI	Ministry of Interior
MS	EU Member State(s)
NCB	National Central Bureau of INTERPOL
OLAF	European Anti Fraud Office
P(C)CC	Police (and Customs) Co-operation Centre
PoA	Principle of Availability
SECI	Southeast European Cooperative Initiative
SI	Swedish Initiative
SIENA	EUROPOL's Secure Information Exchange Network Application
SIRENE	Supplementary Information Request at the National Entry
SIRPIT	SIRENE Picture Transfer
SIS	Schengen Information System
SPOC	Single Point of Contact

1 Executive Summary

In the framework of this study, the status on information exchange amongst law enforcement authorities in the context of the existing EU instruments has been viewed from the perspective of the efficient and expeditious cross-border exchange of information and intelligence within the European Union. The vital importance this holds for public safety has recently been demonstrated again, as media reports of the self declared cessation of terrorist activities by the ETA stressed that its activities had been seriously disrupted by effective cross-border co-operation between Spain and France.

The study was conducted in the context of overarching questions about how much has been achieved in implementing the Hague Programme and what still remains to be done, as well what else needs to be achieved regarding access to and exchange of information among EU law enforcement bodies in order to improve the prospects for EU co-operation in the areas of justice, security and freedom. In this context, the following research questions were at the core of the study:

- Have the Swedish Initiative and the Prüm Decision facilitated the exchange of information and to a sufficient extent?
- To what extent is the Principle of Availability working in practice or is it still only a theoretical concept?
- Which tools of information exchange do law enforcement authorities mainly use, and for which purpose and to what extent? Specifically, what are the roles of EU instruments (e.g. SIS, EUROPOL)?
- How can law enforcement authorities enhance the exchange of information?
- What are the legal obstacles and how can they be resolved?
- What are the technical, practical and operational problems and needs?

Based on the input received from Member States and desk research, a broad view has been obtained on the current status of information exchange amongst law enforcement authorities. It was discovered during the Study that the responsibility for international exchange of information is centralized in most MS, yet local border forces quite often have very significant roles at local and regional levels, even though there are different approaches in different Member States regarding cross-border information exchange at local and regional level. , while this was not the topic of this study, the effectiveness of the structures and the organisation of information exchanges within Member States Law Enforcement Agencies, as well as between agencies within Member States, is very important in evaluating current situations and future opportunities.

The main finding from this study is that the existing cross-border information exchange is functioning reasonably well and that much relevant information is readily available and accessible to law enforcement authorities. However, there is still significant room for improvement regarding co-ordination and standardisation - factors which have an impact on the efficiency and effectiveness of cross-border information exchanges. The existing legal and technical instruments are broadly sufficient and there is no need to introduce new instruments for cross-border information exchange. However, a number of adaptations, clarifications and simplifications are required to ensure that these agreements (legal instruments) and channels (procedures and technical transmission systems) are kept up to date in order to deal with cross-border information exchanges more efficiently and expeditiously. Ensuring proper use of the existing instruments is an especially important priority, as it was found that there are many occasions when legal instruments are not being fully exploited. Where required, the existing tools should be upgraded rather than replaced entirely.

Many MS made it clear that they saw increased co-operation with EUROPOL as vital in the future. Although the role of EUROPOL is becoming more and more important, it should not be forgotten that Europe is only one region of the world; the worldwide police and law enforcement co-operation and exchange of information should, accordingly, not be overlooked. Some MS have certainly recognized the capabilities of institutions such as EUROPOL, INTERPOL, EUROJUST, OLAF, etc. and they provide and share information and intelligence with them to a significant degree.

The Principle of Availability partly works in practice and is certainly a vision worth pursuing. In reality it is almost impossible to realise its full potential - i.e. to exchange information between countries as one would if the exchange were purely within a single country - while there still exist different national, legal and administrative systems, data protection legislations, and also significant interoperability problems. Legal obstacles, which do exist and hamper the efficient cross-border information exchanges, mainly relate to differences in national legislation rather than to the EU legislation.

There are considerable challenges in enabling information and intelligence database material to be fully and promptly accessed within Member States, and made available on appropriately comprehensive bases to other Member States. These challenges include technical IT capabilities, including the availability of encrypted information networks and common or mutually understood security classifications. Work flows within MS are different for a number of good reasons. The information flow to LEAs of other MS also depends on national structures. Nevertheless, there is a potential of harmonisation and gaining synergies without affecting Member States' sovereignty.

It can be established that the Swedish Initiative has not facilitated the exchange of information or criminal intelligence among MS as initially envisaged, with only a few Member States using the Swedish Initiative and its form. In contrast, the Prüm Decision seems to be one of the most efficient tools to identify criminals and solve crimes, although its purpose is not to exchange information or criminal intelligence as such, but enables EU MS to know almost instantaneously if a certain type of information is available in another MS or not. Research done among EU MS indicates that further development should rather go towards the development of new HIT/NO-HIT systems than to opening national databases to other MS law enforcement authorities.

In addition to legal instruments, communication channels, work flows and human factors need to be taken into account. Significant cultural and working practice differences exist within the EU and these differences often have an impact on the approaches and attitudes to cross-border information exchanges. The report highlights Member States' suggestions on how to limit the adverse impacts of these cultural differences, as well as good practices, which might set an example for improved standards in the future.

The main recommendations from this study are that central points of contacts in the MS should be strengthened, and central or common LEA registers at national level should be established for various categories of data without compromising the content (i.e. to ensure data coherence between national agencies in a country and also between MS). For reasons of comparability, also of potentially resulting statistics, such efforts should be coordinated on EU level. There is also a need to speed up the introduction of cross-border secure IT channels in certain areas (e.g. MLA exchange, exchange of documents classified as CONFIDENTIAL, etc.). There should be increased cooperation between agencies on an international level, and the role of EUROPOL and OLAF should be promoted and enhanced, especially on analysis of data and the use of the analysis results by MS. A more pro-active stance to delivery of information by MS should be encouraged in this regard. The exchange of staff among MS should be increased for those officials who are involved in cross-border activities and related information exchange. Pending increased standardisation and harmonisation of legislation, an EU-wide handbook on the procedures related to information exchange could contribute to more efficient work flows.

To conclude, despite ongoing improvements and existing plans for the future, there is still room for significant improvement, especially when it comes to the provision and sharing of information among EU MS law enforcement authorities and multilateral institutions such as EUROPOL and INTERPOL. Currently only a few MS are main sources of data input to EUROPOL's and INTERPOL's databases. Although EUROPOL and INTERPOL have been established to provide services to MS, law enforcement authorities do not yet use their capacities sufficiently. OLAF's AFIS databases have also not received the originally anticipated data inputs from MS. MS should more actively contribute to the further development of those institutions in the future, more clearly express their needs and more frequently ask for their assistance in EU MS operations. The further development of mutually associated projects between EUROPOL, INTERPOL, EUROJUST, FRONTEX and OLAF and the MS presents the greatest challenge for the future, but also the greatest opportunity.

Reference of the contract

JLS/2009/ISEC/PR/001-F3

2 Introduction

2.1 Background

The effective cross-border exchange of law enforcement information and intelligence is paramount for preventing and combating crimes. It is therefore necessary that law enforcement authorities within the EU are able to request and obtain information and intelligence from other Member States in expeditious and effective ways. Co-operation, and exchange of information and intelligence between law enforcement authorities, have to some extent always taken place, whether through informal or formal systems, or through EU or non-EU instruments. Today, the exchange of such data and information and intelligence often takes place on the basis of the EU legislation, and on bilateral or international agreements and conventions, on an increasingly fomalised basis.

Significant progress has been made since the beginning of the 1990s in improving co-operation and exchange of information between law enforcement authorities: The 1990 Schengen Convention, the 1995 Convention on the Establishment of a European Police Office (EUROPOL) and the 1997 Convention on Mutual Assistance and Co-operation between Customs Administrations (Naples II) serve as examples on a European level. At the same time there are many bi-lateral, multi-lateral and regional initiatives in this respect which were established with neighbouring countries across the European Union. Probably the best known and longest serving example of international co-operation is INTERPOL, which since 1923 has been the main global focal point for the exchange of information on international cross-border crime and criminals, and which is still a very important institution within the European Union, although the role of EUROPOL has been strengthened during the last few years.

The Hague Programme introduced the Principle of Availability according to which “the mere fact that information crosses borders should no longer be relevant”. An optimal level of protection in the areas of freedom, security and justice requires multi-disciplinary and concerted action both at national and EU level between the competent law enforcement authorities, especially police, border guards and customs. The Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the EU indicates how to achieve this priority. One of the most important achievements towards implementation of the Principle of Availability is the so-called Swedish Initiative[1], a second important achievement is the Prüm Decision[2].

These Instruments attempt to simplify the exchange of information and intelligence between law enforcement authorities of MS and to step up cross-border co-operation, particularly in combating terrorism and cross-border crime. The latest development in the field of law enforcement co-operation came with the Lisbon Treaty, which specifies that the European Union shall establish police co-operation involving all Member States, including police, customs and other specialized law enforcement services, to address the prevention, detection and

[1] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the MS of the EU

[2] 2008 Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p.1

investigation of criminal offences. An important recent step was also made with the "Stockholm Programme" in the course of the Swedish Presidency of the EU. The Stockholm Programme, which was endorsed by the European Council in December 2009, determines work in the area of justice and home affairs in a five-year programme and acknowledges the need for coherence and consolidation in developing information management and exchange.

The Hague Programme, the report of the Future Group of Ministries for Home Affairs, the Stockholm Programme and several other documents have highlighted the need for coherence and consolidation in developing information exchange in the field of EU internal security[3]. In order to reach that strategic objective, the European Information Exchange Model seeks to map, assess and recommend ways to consolidate the cross-border exchange of information and criminal intelligence in the field of EU internal security. This Study contributes and complements the European Commission's exercise and its four maps on legislation, communication channels, information flows and technological solutions, respectively.

2.2 Objectives of the study

All the above-mentioned legal acts and institutional measures may be insufficient if there exist hindrances to an effective and efficient exchange of information and intelligence. In this context it is also important to review what and how much has been achieved in implementing of the "Hague Programme" and what still remains to be done. One aim of the study was to participate in the preliminary evaluation process of the "Swedish Initiative" and the "Prüm Decision" by analyzing data from MS on the operational efficiency of these instruments.

The objectives and scope of the study have been devised to support the European Commission in its endeavour in the development of the European Information Exchange Model and its four maps, specifically focusing on Communication Channels and Information Flows. The findings of the study should underpin, support and complement the European Commission and the Council Ad Hoc Working Party on Information Exchange in implementing the aims and objectives of the Information Management Strategy. In line with the Information Mapping Project of the European Commission, the Study's scope was restricted to information exchange for the purpose of criminal investigations and criminal intelligence operations in the pre-trial phase in the EU and with the four EFTA countries.

The main objective of the Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments was to identify and analyze the current situation with regard to cross-border exchange of information across the EU Member States, identifying gaps, shortcomings and redundancies, and to provide an analysis of the needs of law enforcement agencies and identify means to meet these needs. The study therefore points out the achievements in implementing the Hague Programme and what still remains to be done, as well as what other measures are required in the area of access and exchange of information among EU law enforcement authorities in order to improve the prospects for the European Union in the areas of justice, security and freedom.

[3] "Council Conclusion on an Information Management Strategy for EU internal security", 2979 JHA Council meeting, Brussels, 30 November 2009 (doc. 16637/09 JAI 874 CATS 131 SIM 137 justciv 249 JURINFO 145)

2.3 Methodology

The study's methodology has been tailored to meet the objectives described above. It was important to take into account the situation in all 27 EU Member States and the various national authorities considered part of the law enforcement system. At the same time, it was not feasible within the budget and time constraints to cover all of them in the depth necessary for a detailed process, gaps and needs analysis. The Project attempted to address this quality vs. quantity question by following a dual approach, firstly by collecting information via a questionnaire from all 27 Member States[4], and secondly by conducting in-depth research and process analysis in a carefully selected set of 12 out of the 27 Member States. These Focus Countries have been carefully chosen in order to provide geographical spread (north/south, east/west), various regions (Central, Eastern and Western Europe, Balkan, Scandinavia, Baltic, Mediterranean), various traditions in law enforcement (centralized/decentralized), different types of borders (External EU and Schengen border, sea borders, land borders), different type of MS (old MS, new MS and non-Schengen MS) and different legal bases (Civil law/Roman law).

Table 1: Countries Visited

Focus Country	Agencies consulted
Austria	• Ministry of Interior/Directorate for Public Security • Bundeskriminalamt – Federal Criminal Investigation Service • Ministry of Finance/Customs Administration
Slovenia	• Ministry of Interior/Police Directorate • Ministry of Finance/Customs Administration
Finland	• Ministry of Interior/Police and Border Guard Departments • Ministry of Finance/Tax Department, Customs Unit
Italy	• Ministry of Interior/SCIP Office • Carabinieri
Netherlands	• Politie – National Police Agency • Royal Military and Border Police • Customs • Police
Estonia	• Estonian Police Board • Estonian Board of Border Guard • Estonian Tax and Customs Board
Bulgaria	• Ministry of Interior/General Directorate Fight Against Organised Crime • Ministry of Interior/General Directorate Border Police • Ministry of Finance/ National Customs Agency
Greece[5]	• Telonia – Customs • Limeniko – Coast Guard
France	• SCCOPOL • Direction Centrale de la Police Judiciare – Judicial Police • SCTIP • Douanes – Customs
Germany	• Ministry of Interior • Bundeskriminalamt – Federal Criminal Police Office

[4] Answers to the questionnaire were received from all EU MS but Portugal

[5] The Greek Police only participated as observer during the third day of the visit

	• Landeskriminalamt – Regional Criminal Police Offices Wiesbaden and Meckenheim • Federal Ministry of Finance • Zollkriminalamt – Customs Investigation Service
Denmark	• Rigspolitiet - National Police • Ministry of Justice
United Kingdom	• Ministry of Justice • Home Office • National Policing Improvement Agency • Central Authority for Exchange of Criminal Records • Serious Organised Crime Agency • Greater Manchester Police • Kent Police • UK Border Agency • HM Revenue and Customs

A draft questionnaire was developed by the project team and later revised in the light of EC and EUROPOL comments, as well as comments from the Austrian law enforcement authorities who were piloting the methodology of the study. Before dissemination to all 27 EU Member States the Information Mapping Project Team[6] provided additional feedback in order to identify and eliminate possible weaknesses and to ensure commitment of the MS involved in the Information Mapping Project Team. The questionnaire, attached as Annex 1, contained largely general questions as the questionnaires were delivered to different law enforcement authorities dealing with the exchange of information across the EU. The Study targeted the main law enforcement agencies in each country, which in general are police (including border police) and customs authorities. The difference in national structures, leading to very different national law enforcement authorities providing answers to the questionnaires (see Annex 2), naturally restricted the comparability of data. Where appropriate, distinctions were made between police and customs replies as in many cases Customs Services provided their own replies to questionnaires and were met separately in the visits to the Focus Countries.

The purpose of the general questionnaire was to receive a response from all 27 Member States with adequate information to form the basis for the comparative analysis. In order to ensure an adequate response rate, the questionnaire was designed to cover all relevant aspects of cross-border information exchange, while not requiring excessive time input by the respondents. For reasons of comparison, and in order to assess the Principle of Availability, co-operation between those law enforcement authorities on a national level was also examined. The questionnaire focused on the level of international exchanges, work flows and problems faced in the cross-border exchange of information. Next to the generic description of business processes, three carefully engineered case studies regarding the exchange of information were included in the questionnaire to achieve a preliminary contextual understanding of the work flows involved. The purpose of including of the case studies was to get a clear and realistic picture of the information exchange, communication channels and information flows at international and national level. The following three topics were chosen as a basis for case studies in view of the comments received from the Information Mapping Project Team:

[6] The Information Mapping Project Team is made up of Member State representatives, EUROPOL, EUROJUST, the EDPS, and FRONTEX, coordinated by DG HOME

- Trafficking in Human Beings, including child trafficking for the purpose of begging
- Drug smuggling and trafficking of stolen vehicles
- Computer-related crime (phishing)

Structured interviews in the Focus Countries were an opportunity to verify the information from the questionnaires and gain further insight into the processes of international information exchange in those countries. This approach ensured that a strong factual and analytical accuracy was presented in the study for the selected, representative Focus Countries, while at the same time providing a comprehensive picture of the situation in the entire EU.

In each of the Focus Countries a small team of key experts - subject experts on police (including border police) and customs matters, as well as a process analyst - made visits and conducted interviews and research. The experts studied the replies to the general questionnaires in advance of their visits. In contrast to the general questionnaire, the Interview Guide, upon which the structured interviews in the Focus Countries were based, contained detailed and analytical questions regarding operational level issues and especially work flows. It also required more precise information on the levels and ratios of exchanges with other Member States, and on what type of information is requested or is being provided. Open questions were asked regarding any specific needs, problems or issues regarding redundancies which the authorities might have or be aware of. The focus and awareness of practical difficulties in exchanging information may differ between the strategic/management and operational level. For that reason both managerial and operational officers in Member States were targeted for interview and discussions in the Focus Countries. Furthermore, on a few occasions local level officers participated in the interviews. In addition, sample Co-operation Centres were visited at Thörl Maglern in Austria (Austria, Slovenia and Italy) and Heerlen in The Netherlands (The Netherlands, Belgium and Germany).

The generic Interview Guide was presented to the EC before the first mission of the expert team. Prior to the country visits the subject experts adapted the Interview Guide in accordance with their findings from the background research and legal and literature review, as well as the feedback received from the general questionnaires. The answers to the interview questions, as well as the description of the work flows involved in international information exchange, were noted down by the experts during the interviews, and were sent to the participants of the interviews for further comments and validation. The validated Interview Guides for the Focus Countries can be found in the Country Reports annexed to this study for reference. Access to the law enforcement authorities was greatly facilitated through the members of the Information Mapping Project Team, and in most countries also the presence of a “National Facilitator” – a person with contacts in and knowledge about the law enforcement authorities in his/her country.

Further to the MS’ views, it was very important to get institutional views on the current status of the cross-border information exchange within the EU. For this reason, the Project consulted relevant organizations such as EUROPOL, INTERPOL, EUROJUST and OLAF.

2.4 Terminology

2.4.1 Law enforcement authorities

While law enforcement authorities in general can be described as authorities responsible for upholding law and order, in practice EU MS have very different national law enforcement systems in place. They 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. For the purpose of this study the national members of the Information Mapping Project Team were asked to identify their respective national law enforcement authorities for forwarding of the questionnaire and for invitations to interviews in the Focus Countries.

2.4.2 Information and intelligence

There are various ways in which Member States understand the terms "information" and "intelligence". Central European countries mostly use the term »information« while English speaking countries use both "information" and "intelligence" and make distinctions between them. In order to provide a common understanding of the definitions, a short explanation and reference needs to be given. While the definition of "information" is relatively straightforward, the Hague Programme or subsequent EC policies and legislation offer little guidance in the definition of "intelligence". In Article 2(d)(i) of Council Framework Decision 2006/960/JHA (the Swedish Initiative), "information" is defined as "Any type of information or data which is held by law enforcement authorities" and "intelligence" is defined as "Any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures…". There is a question of whether this definition provides a precise and operational definition of intelligence. It seems that information, to be called intelligence, needs to be qualified, enhanced and improved, i.e. that a piece of data or information in itself is not intelligence until it undergoes some sort of processing and analysis. Intelligence can be therefore seen as information which is significant or potentially significant for an enquiry or potential enquiry. In line with this, "intelligence" could be defined as "information which has been evaluated and analysed and which had been identified as being of material value or potential material value".

In civil (Roman) law a distinction is usually made between the "intelligence" or "pre-investigation" phase or inquiry where police officers have autonomy, aimed at establishing whether a crime has been committed, and the "investigation proper" where magistrates or prosecutors take command. Information and intelligence can be obtained from other international law enforcement authorities, but once a formal investigation is launched by involvement of a prosecutor, the use of a Rogatory Letter is required. Information that is internationally exchanged can only be used as police information and not as evidence in judicial proceedings. In contrary to civil law, in common law systems such as that of England, Wales and Northern Ireland, law enforcement officers have greater responsibilities for investigations and a Rogatory Letter is always required for the evidence to be produced in court.

2.4.3 Information and IT Channels

A lot of confusion is caused by using the same or similar wording for different meanings. For example, when using the term ‘information exchange channel’ one means the procedural administrative routing regardless of technology, whereas others understand the IT channel being used. Similar to this, the word ‘network’ may be understood as an IT term (wired telecommunication lines), whereas others just mean a link and co-operation between certain authorities or even single persons.

As a result, even more misunderstanding is caused by the use of different IT channels. When technicians speak about the INTERPOL channel, they probably mean the I-24/7 IT network of INTERPOL. This does not imply that the INTERPOL General Secretariat would receive and store the information, as I-24/7 also acts as a relay from one member country to another. In other words, the information is merely sent over the INTERPOL dedicated data lines without storing the content of the information at IPGS.

The same applies to EUROPOL. When someone asserts that information will be sent to EUROPOL, it is often unclear what it means in practical terms. It can mean that a Member State’s ENU sends information to their ELO or to EUROPOL staff or to the only recently established 24/7 service (EUROPOL SPOC). EUROPOL’s secure IT network can also serve MS just as a relay and messaging service between MS without storing the content of the information (similar to INTERPOL). If chosen and implemented by MS, the EUROPOL network application SIENA provides end-users with an IT messaging and documentary client application and, if desired, interfaces for direct consultation with EUROPOL’s information system databases (EIS). Due to the fact that SIENA is still in the roll-out phase and MS can opt which part to use, some MS use only certain parts, whereas others use it to its fullest extent.

Regarding the terminology in this text, we try to overcome the problem of misinterpretation by using terms such as ‘information cannel’, ‘exchange channel’, ‘network’, etc as a logical and procedural term regardless of the technical means used. Where we refer to information technology, meaning a physical IT network, we will add the term IT for clarification.

Another example is the term ‘access’, especially in the context of access to systems and databases. For good reasons internal or external personnel responsible for data protection monitoring and enforcement are often alert to possible administrative or legislative breaches when someone says that agency X needs access to a certain IT system. However, a request for access does not necessarily specify to which level, and by which means, access is obtained. For example, access can be given by user permissions in a way that a user would use a client application from a PC and connect to the database. This still does not say which details of results a user would receive. It can be a simple YES/NO indication or limited information and saying that the case leading agency should be contacted, or it can be any other level of detail. On the other hand, even common email services, without direct connectivity to a database, can mean ‘access’. For example, if an email is generated as request and the partner system automatically processes the inquiry and responds to the sender, there is not much difference to the example above. (i.e. simple, automated, YES/NO information). The level of information responded to the requesting party is under full control of the database owner by specifying the conditions of the response. This can range from denying access (e.g. because the originator could not be validated) to several levels of information to be provided in response.

Furthermore, user permission will also manage the kind of transaction to be processed. Retrieval requests (show me specific data in response), update requests (correct or amend an existing record) or deletion requests (remove the record from database) are quite different in nature but can be initiated by all means. In summary, the word ‘access’ does not say anything without detailing what to achieve. When we are using the term ‘access’ without detailed specifications in this document, we mean a direct IT channel (ideally on-line) and that a request should result in an immediate response. This specifically also relates to the references throughout this Study to establishing “registers” which enable all agencies to have immediate “access” to the existence of records, where at this stage it is open what would be held within those records.

3 Identification and analysis of current exchanges of information

Cross-border information exchanges between law enforcement agencies encompass different types of information exchange. The most well-known are traditional exchanges of information and intelligence on persons, vehicles, firearms, financial and communication data, etc. via different communication channels (INTERPOL, EUROPOL, SIRENE, etc). Of increasing quantitative and qualitative importance is the automated comparison of data, and also identification on "HIT/NO-HIT" systems. These two latter categories cannot be literally seen as information exchange, but create bases for further information exchange or mutual legal assistance and give added value to cross-border information exchange and law enforcement co-operation. Information and intelligence, as a rule, are mainly exchanged via national central authorities or national contact points (INTERPOL National Unit, EUROPOL National Unit, SIRENE) and the communication channels used are very often combined and complemented with different types of additional channels (Police and Customs Co-operation Centers, Police Co-operation Centers, Liaison officers, Joint Investigation Teams, etc.).

This chapter aims to provide an overview over the current status of information exchange between LEA in EU MS, starting from the national structures in place in MS for international exchange of information, to the legal bases upon which information is exchanged, the scale and types of information exchanged, to the variety of channels available for such exchange. The last sub-chapter provides a short analysis of the main work flows involved in cross-border information exchange based on the Focus Country interviews and the answers to the questionnaire related to the case studies.

3.1 National Structures

MS have set up different national structures for cross-border information exchange, which often have significant influences on the efficiency and effectiveness of such exchanges. This not only relates to the division of law enforcement tasks between various agencies, but also to the set-up of the individual agencies themselves.

Single Points of Contact (SPOCs), created at national levels, seem to be one of the most efficient tools for cross-border information. In some countries national offices for particular exchange purposes (e.g. NCB, ENU) are separated from each other, while in other countries this is not the case. In Germany, Denmark and Estonia, for instance, officers act at one time as NCB and at another time as ENU. In almost all visited MS, simple requests from other MS can often be answered by SPOCs of individual national law enforcement authorities holding necessary information or criminal intelligence or having access to relevant registers or databases without recourse to other agencies.

Generally all MS have good 24/7 contact organisational structures. However, this does not necessarily mean that all national agencies within a country have such structures in place. Some may be reliant on other services, typically the national (usually police led) SPOC. Proposals for upgrading SPOC roles and capabilities need to be clear about definitions. Some 24/7 SPOCs have full staff support facilities whereas others are night watchmen services which are fully adequate for HIT/NO-HIT requests but not necessarily for more resource intensive information or assistance requests.

The large MS have widespread agency or multi agency SPOC capabilities at national central level, whether in centralised (e.g. France), regionalised (e.g. UK) or federal (e.g. Germany) states. However, it was clear that despite their larger resources all the larger states are heavily dependent on SPOCs (national and regional) or their near equivalents, and P(C)CCs, which could be considered SPOCs on regional and local levels. Visited MS felt there were significant gaps in the overall awareness of national structures of other MS, which could be filled by a number of co-ordination/co-operation measures, such as mutual exchanges of information on operating procedures (e.g. instruction manuals), and by exchanges of professional SPOC and P(C)CC staff.

Not surprisingly, the structures of the centralized authorities for cross-border exchanges largely depend on the governing structure of the country in general. In some EU MS there are highly centralized state structures (e.g. France, Slovenia) whereas in other countries federal systems and different police sub-systems are in place (e.g. Germany, Spain). In practice, different units and agencies are dealing with different parts of the police and other LEA co-operation at national levels and therefore accessibility through a single point of contact is necessary; a requesting country should not have to take responsibility for dealing with differing competencies and relationships in the receiving MS. The responsibility for the co-ordination of competencies should lie with the receiving country, although the requesting country should of course update its procedures after being informed of the correct competent authority in the receiving state.

The descriptions below of Focus Countries structures make it clear that there are significant differences between MS regarding the responsibilities of agencies, and not just between police and customs. All MS stressed that it is therefore vital that the purpose of requests, and the use to which replies will be put, must be clearly explained. It is not realistic for the organisational structures of other MS to be easily explained to all necessary LEA staff in the requesting or supplying MS. The good practice in several MS visited is to forward the request to the correct receiving authority while replying to the requesting MS that this has been done, together with full contact details of the new receiver. This is felt to be a mutually effective approach.

MS are generally increasing the domestic levels for all agencies to gain greater access to investigation and intelligence data, either by mutual interchange, or the creation of common databases to which all agencies have full access or are able to view basic HIT/NO-HIT data and further information relevant to their jurisdiction, with degrees of automatic notification to the creators or overseers of the data. This common internal database development, described in greater detail in the following overviews of the Focus Countries, is a crucial progression in the enhancement of external exchanges with other MS and should be further encouraged, with the technical developments and corresponding uses and human resource training being disseminated to other MS so that positive and negative experiences are widely understood.

Evidence given by Focus Countries on the domestic increase of the direct integration of national databases (Slovenia, Finland, Estonia, Denmark and UK) and also indirectly through domestic

LOs (from other national agencies) in SPOCs, or centralisation of regional forces (Netherlands) or through cross agency regional co-operation (France, Germany, Austria) support the argument for database integration. To avoid misunderstandings, this does not necessarily mean that databases would be merged into one huge database. Nevertheless, there is a demand for greater harmonisation of existing information sources and easier access to them, and at the same time for reliability, relevance and accuracy of that information. In other words, it is important to know where the same information is stored and when one database is updated by one stakeholder (e.g. OLAF's) how and when this corrected and most recent information would be shared and amended in other databases (e.g. SIS). Otherwise LEA officers will get data from different sources, and if key information, such as names or company details vary, even though it is from the same case, a lot of effort is required to clarify which information is correct.

The position of Border Guard or Border Police services warrants some specific comments. In comparison with other agencies, particularly Customs, these services have a greater need to near instantaneous access of data from their own countries' agencies, or from other MS. Notwithstanding the fact that border police authorities are playing important roles in tackling cross-border organized crime, their share in the overall information management is relatively small compared to other major agencies, such as Police or Customs. These authorities are mainly tackling illegal migration, fighting against trafficking of human beings and document falsification. When it comes to information exchange on intelligence, independent border police authorities are facing the same challenges as general police authorities as described in the study.

In some EU Member States border police authorities are independent from the general police, while in other MS these authorities are integrated into the police system. In those EU countries where border police/guard authorities act independently from the general police authorities, adequate inter-agency agreements (legal and sub-legal acts) exist to facilitate intelligence information exchange.

The integration of independent border police authorities into general police structures and the concomitant procedures, which do not always respect the existing communication channels, could potentially lead to loss in the flow of information. When institutional changes occur, special attention should be paid to maintain the already existing structures of information exchange. The merging of two agencies may result in a more streamlined organizational body, but the flow of information has to be secured by ensuring the necessary human and technical resources above the legal and institutional backup.

Border Guards' Rights to investigate criminal cases also differ in each country, which affects their role in the intelligence cycle. Usually border police/guard authorities have either limited or even no investigatory rights provided by the respective national legislation, therefore narrow access to the police channels are experienced. Due to the specific nature of their work, border police authorities have frequent direct access to SIS, liaison officers, police and customs co-operation centres, FRONTEX information and analytical sources, FADO. In all other cases the central unit responsible for international information exchange creates a bridge between the border police and other Member States/Institutions. It has to be noted that border police authorities often are not fully aware of the potential in using the police channels. Even if they are aware of their existence, adequate knowledge is missing about how they function, and what the common procedures are; this may well cause delays or deviation in the information cycle.

Although it is difficult to compare differing structures due to different legal, historical, geographical and structural backgrounds, structural overviews of the national law enforcement structures in the EU MS are given below. Naturally, the descriptions of the visited Focus Countries are partly more detailed, as the summaries on other MS are purely based on the information provided by them in the answers to the questionnaires. Further details of the situations in the Focus Countries are to be found in the Country Studies in the Annex. Despite the apparent differences, the challenges and opportunities were perceived to be basically similar in the Focus Countries and based on the answers to the questionnaires can be assumed to be so also for the other MS.

In Austria the central authority for exchange of information and intelligence is the Criminal Intelligence Service (Bundeskriminalamt - .BK). The .BK acts as the NCB, ENU and SIRENE unit(s) and is responsible for international information exchange irrespective of the subject matter with the CIS Telecommunications Centre and registration sub-unit acting as a central receiving point for requests from abroad (EUROPOL, INTERPOL, SIRENE), forwarding messages to SPOCs of relevant agencies, who then route to specialized units and vice versa. Customs exchanges are the responsibility of Dept. DG IV/3 of the Finance Ministry. Customs has full investigatory roles in relation to customs, excise duties and tax, although prohibitions such as drugs offences are dealt with by the police. DG IV/3, which acts as a SPOC, has a fully internally integrated capability with investigators, analysts and legally trained staff being collocated. The Customs Liaison Officer at .BK is responsible for co-ordination with BKA and INTERPOL / EUROPOL.

In Belgium the police are structured federally and locally. The Federal Police and the extensively used P(C)CCs and PCOs (operational contact points) with neighbouring states are under the Interior Ministry, with Customs under the Finance Ministry. The Federal Police CGOT (Service for Handling of Operational Information) includes national and international contact points (NCB, ENU, and SIRENE) and is responsible for national management of information including the ANG general national information and intelligence database, coordination with P(C)CCs in the border areas, and for strategic analysis of crimes. At both federal and local level there are sub-national information centres (AIK) which have local databases. AIKs are responsible for processing information and inputting into the ANG. Customs is extensively involved in international exchanges through CGOT and its involvement in the PCCCs as well as with OLAF and MS through the CIS and other AFIS systems.

In Bulgaria the International Operational Police Co-operation Directorate (IOPCD) is a central unit responsible for cross-border information exchange. Within the structure of the Directorate are the NCB, ENU, SIRENE Bureau (Bulgaria is scheduled to join the Schengen Information System in October 2010), as well as a unit responsible for exchanges under bilateral co-operation agreements. IOPCD's Telecommunication Centre operates as 24/7 SPOC. The General Directorate for Combating Organized Crime (GDCOC) acts as a SPOC with relation to information exchange with countries which are members of SECI Centre, and for cyber crime. The Customs Service does not have investigatory powers – these and related information exchanges are carried out by other agencies, especially the GDCOC and onwards to the IOPCD, although administrative assistance requests are exchanged directly by Customs and these often migrate to criminal investigation cases. The responsible section in Customs is the Information Exchange Unit of the Intelligence and Investigation Dept. of the Central Customs Directorate which is especially responsible for input to the OLAF AFIS systems. Given the extensive heroin trafficking challenges in Bulgaria, the anti drugs unit often deals directly with MS through very regular liaison with the significant number of MS LOs in Bulgaria. As with other agencies, Customs expect considerable qualitative and quantitative benefits from new P(C)CCs with Greece and Romania as well as, in the future, with Serbia.

In Cyprus the Cyprus Police is responsible to the Ministry of Justice and Public Order (MOJPO). The Police Cooperation Office - European Union and International Police Cooperation Directorate (ENU & NCB) is responsible for cross-border information exchange. In addition, the Unit for Combating Money Laundering (MOKAS), the Office of Attorney-General of the Republic and the Department of Customs and Excise under the Ministry of Finance are also involved in cross-border information exchange.

In the Czech Republic the Police are responsible to the Ministry of the Interior, and the Directorate General of Customs and Customs Headquarters are responsible to the Ministry of Finance, with the Military Police reporting to the Ministry of Defence. All police agencies are divisions of the police itself rather than separate agencies. The police have collocated units for international exchanges – National Exchange (NE) SIRENE in relation to SIS and operation of the European Arrest Warrant, the NCB, for EU MS exchanges not specified by SIS, and the ENU. The International Cooperation Division (IRD) in the same national HQ coordinates the flow of information from regional and local centres, including the P(C)CCs, and exchanges made by specialist police divisions which have national responsibilities (National anti-drug centre, Division for the exposure of organised crime, Division for the exposure of corruption and financial crime). There is a shared information and intelligence database for NE, NCB and ENU but this is not widely available to other units and work is being done to make it so. Police have access to non police databases including those registering citizens and vehicles. Customs have equivalent powers to the police in relation to Customs matters with their own databases. The national co-ordination unit of the Directorate General of Customs is Section 313 - the Central Coordinating Unit for implementing the Convention on mutual aid and co-operation between customs agencies of the EU. It deals with such exchanges centrally and has a representative at EUROPOL. Customs staff also participate with police at the five PCCCs.

In Denmark the National Centre of Investigation (NCI) is responsible for national co-ordination and international exchanges. The Communication Centre, which is set up within the NCI, is responsible for correspondence through the SIRENE, INTERPOL and EUROPOL channels and to the local Police Districts. All incoming and outgoing communications go through its 24/7 SPOC, which co-operates with Ministry of Justice, Customs and Taxation Authorities, Ministry of Foreign Affairs, Immigration Service, Danish Embassies, and acts as a central register office. Operationally, NCI acts as the sole focal point and work is carried out for the Danish police, the Nordic Police and Custom Co-operation Network (PTN), and with INTERPOL, EUROPOL and FRONTEX, etc. NCI staff are not separated into different departments, are empowered to, and expected to, work on cases for any channel, and have full access to national intelligence and investigation databases. International requests or responses to incoming requests from abroad are prepared by NCI directly, or indirectly by reviewing all requests or replies which are prepared elsewhere (e.g. in specialist units or Regional Police Units).

In Estonia the Criminal Intelligence Bureau (CIB) of the National Criminal Police fulfils the tasks of the SIRENE Bureau, ENU and NCB and co-ordinates information exchange with liaison officers; all tasks being integrated into one common service. The preparation of a request can be done either by regional case officers or by the CIB. There are also cases that are dealt with centrally by the National Criminal Police. The Tax and Customs Board (TCB) has full investigatory powers and has a Customs Officer based at EUROPOL. The International Co-operation Unit of the TCB Investigation Dept. acts as the SPOC for international exchanges, on a 24/7 basis. There is extensive co-operation with the CIB through the TCB Liaison Officer, and with the Nordic PTN network either directly or through the Finnish Customs LO based in TCB. All relevant agencies have access to the joint investigation and intelligence database (KAIRI).

In Finland the Communication Centre of the National Bureau of Investigation (NBI) processes all international communication to and from Finland and makes preliminary checks on all incoming messages, passes information on for further measures (e.g. to Mutual Legal Assistance section), inserts information into the data systems of Finnish Police, performs SIS quality control and co-operates with Customs, Border Guard and immigration authorities. It functions as the SIRENE office, ENU and NCB and as a central registration office. Simple requests are processed by NBI themselves, while in other cases requests are distributed to relevant agencies. Finnish Customs have full investigatory powers and regularly exchange intelligence with CIS and other AFIS systems. It also, together with prosecutors, exchanges judicial co-operation requests with MS directly. Like the other Finnish services, information is often passed formally after informal contacts through the PTN Nordic Liaison Officer Network. There are also widespread contacts with customs and police staff of neighbouring countries on an informal basis on urgent matters. There is extensive cross agency internal liaison within Finland through the national and Regional PCB Units (Police, Customs and Border Guards). Key data is shared for entering into the main information databases of various services (Police into Customs and vice versa). An all agencies intelligence database will be introduced in the next few years.

In France SCCOPOL is a special inter-ministerial unit within the Central Directorate of the Judicial Police. SCCOPOL manages and co-ordinates the international police co-operation channels: INTERPOL, EUROPOL, Schengen and Prüm, from an operational point of view, housing personnel from the National Police, Gendarmerie, Customs and Magistrates, as well as translators. The SPOC placed within SCCOPOL is responsible for handling incoming requests to and from the French units abroad (from National Judicial Police, Local Judicial Police, Gendarmerie, Customs, local public security police forces, International Department). Requests to and answers received from other countries are sent directly to the respective services (international relation officers) within SCCOPOL. The SCTIP (International Technical Police Co-operation Service) is a section of the General Directorate of the National Police. One of the main tasks of the SCTIP is to exchange information and intelligence with foreign authorities by use of French liaison officers and attaches abroad, through a 24/7 duty office which provides contacts between the relevant directorates and services of the National Police and Gendarmerie. The Customs Service has its own communication channels as a fully empowered LEA. In addition to a liaison officer at SCCOPOL, it has a similar information exchange structure. The SNDJ (National Judicial Customs Service) is the investigating arm and is responsible for taking action and requesting judicial co-operation in conjunction with the examining magistrate. It is supported and complemented by the DNRED – National Customs Intelligence and Investigations Directorate - which receives and sends non judicial requests and replies and provides a SPOC (replicated regionally) for the entire Customs service.

In Germany the Bundeskriminalamt (BKA) houses the NCB, ENU and SIRENE office, and also represents the 'Prüm authority'. The national offices (NCB, ENU) are not strictly separated from each other and BKA officers act in different roles. At the domestic level the BKA ensures the flow of information from other countries/organisations to state police, customs authorities and the Federal Police, as much police activity falls under the responsibility of the 16 'Länder'. Incoming requests from abroad are received by a permanent 24/7 SPOC service (ZD11 of the BKA) and forwarded to ZD21 where the case is registered. Depending on the details of the request, the response is either generated by the BKA directly or the request is forwarded to the appropriate authority within Germany to obtain facts or details. Although the BKA has access to its own nationwide databases and to certain information of 'Länder' cases, the details of cases can only be retrieved by the respective 'Land'. In general the process is the same for evidence and intelligence/information although in some cases Judicial Assistance may be required. In the Länder, the Landeskriminalamt (LKA) is the police authority checking validity and quality, with BKA doing final checks and forwarding to MS or seeking further details from the LKA. The ZKA (Zollkriminalamt) is the investigative arm of the (Federal) Customs Service and is organized on similar lines to the BKA, although there are no Customs Officers under the authority of the Länder. The ZKA has a SPOC and a specialized Section (Section 3) dealing with international and EU co-operation. ZKA Section 3 has a sub section - the Mutual Assistance Team dealing with the handling of international requests, and often preparing and answering them. Other sub-sections deal with specialized drugs trafficking issues and with major cigarette smuggling and other large scale frauds such as heating oil smuggling. These Sections often deal directly with their MS counterparts and with EUROPOL, where ZKA has an officer in the German NU. The Mutual Assistance Team ensures that all exchanges are registered and appropriate information entered into ZKA's information and intelligence databases and those of BKA, with whom liaison is continuous.

In Greece the Ministry of Civil Protection (previously the Ministry of Interior, Decentralization and E-Governance) is responsible for police forces and coordinates international cooperation through the International Police Cooperation Dept. (IPCD) which houses the ENU, NCB, SIRENE Offices and the Drugs Coordination Unit. The Coastguard under the Ministry of Maritime Affairs, Fisheries and Islands also has staff seconded to IPCD as does Customs, under the Ministry of Finance, and several other financial and anti money laundering investigation and intelligence agencies such as the Financial and Economic Crime Unit, and the Anti-Money Laundering and Anti-Terrorism Financing Commission, also under the Ministry of Finance. There is a special Coordinating Body for Combating Drugs (S.O.D.N.) and the S.O.D.N. has been appointed to act as the National Intelligence Unit (EMP) for drugs trafficking issues, with members of the police, Coastguard and Customs on its co-ordination committee. All agencies similarly liaise with the Special Investigation Service, which has responsibility for dealing with complex international organised crime matters, and which includes former Tax Service and Customs Service staff. Each Regional Police Division has a unit reporting to the IPCD-based Centre for Managing and Collecting Operational Information and similar structures exist within the Customs and Coastguard. These Centres have particular responsibilities for preparing requests and replying to requests in relation to cross-border information exchanges for forwarding to the IPCD. Customs has staff seconded to each relevant section of the IPCD as well as to EUROPOL. Customs maintains its own EU wide intelligence links through direct inputs into CIS and other AFIS databases. Cooperation with FRONTEX (by police and Coastguard) is increasing with consideration being given to setting up a FRONTEX sub-office in Greece. Police and Customs have staff at SECI Centre and a P(C)CC is in the process of being introduced with Bulgaria.

In Hungary the Hungarian National Police (under the subordination of the Ministry of Interior) and the Hungarian Customs and Finance Guards (under the Ministry of Finance) are responsible for information exchange on law enforcement issues. Central, regional and local units are controlled centrally and report information for international exchanges to their respective centres. Under the Police structure the ILECC (International Law Enforcement Cooperation Centre) is responsible for exchanges of criminal data but does not have investigation authority itself, therefore enabling it to concentrate on exchanges and information recording. It houses the SIRENE and INTERPOL National Bureau and the EUROPOL National Unit. Urgent exchanges can be done directly at local level (e.g. at the P(C)CCs) but ILECC must be notified. P(C)CCs (also known as International Common Contact Offices) are in place with Austria, Slovakia, Slovenia and Romania. Specialized Divisions particularly involved in liaison with ILECC include the Organised Crime Coordination Centre (analysis work), the Assets Recovery Office (ARO) of the National Bureau of Investigations and the Dept. of Prominent Migration (also called Organized Immigration Crimes Unit). Investigation and Prosecution (Robatzsaru) and Intelligence (TIAR Classified) databases and related communications system are centralized with nationwide access which limits the duplication of communications.

In Ireland An Garda Siochana (the Irish Police Service) is responsible to the Department of Justice & Law Reform. Customs is a component of the Revenue Commissioners, responsible to the Department of Finance. The National Criminal Intelligence Unit (NCIU) is the domestic and internal unit responsible for information exchanges, co-ordination and collation and analysis. All exchanges of criminal intelligence with external LEAs on serious crime or major criminals are also notified to the NCIU which acts as the national SPOC. The international exchange unit is the Garda Liaison Section, which co-ordinates the activities of NCB, ENU and the Garda International Liaison Officer network in MS. There is an integrated national investigation and intelligence database PULSE (Police Using Leading Systems Effectively). All information/intelligence coming to the notice of any member must be recorded on PULSE or, where information is deemed too sensitive, must be made available through defined processes. There is an operational protocol in place between the Garda National Drugs Unit and the Customs CDLE (Customs Drugs Law Enforcement Division) responsible for prevention of drugs importation. Customs have an officer assigned to the ENU and to EUROPOL HQ, alongside Garda colleagues. There are extensive informal liaison contacts between both services. Customs main bodies involved in international exchanges are the Investigations & Prosecutions Division, Customs Investigations (CEIB) and CDLE, responsible for Naples II and MLA exchanges respectively regarding revenue (fiscal customs) offences, and drugs and other prohibition offences respectively.

In Italy the Service for Police International Co-operation (SCIP) of the Criminal Police Central Directorate is the office and contact point for exchange of information to and from EU Member States. The SCIP includes INTERPOL, SIRENE and EUROPOL offices and supports national law enforcement agencies in the international information exchange (State Police, Carabinieri Corps, Guardia di Finanza, Penitentiary Police and State Corps of Foresters). Other national agencies (e.g. DCSA – Central Directorate for Anti-drugs Services) directly liaise with foreign counterparts on their own specific matters. International requests or responses to incoming requests from abroad are prepared by SCIP case officers in relevant units. The front desk is being upgraded to a full one stop shop. The role of the Customs Service is somewhat different from many other MS as responsibilities for Customs matters are shared with the Guardia di Finanza. Both Customs and the Guardia, however, do have direct exchanges with MS and OLAF in relation to AFIS systems, and maintain their own intelligence and information databases while ensuring that key relevant information is recorded with SCIP as the national "central register". Both services participate in the manning of P(C)CCs with France, Switzerland, Austria and Slovenia.

In Latvia the State Police and Security Police are responsible to the Ministry of Interior. The Finance Police Board and the Customs Criminal Investigation Board are both part of the State Revenue Service responsible to the Ministry of Finance. All these agencies and the separate KNAB (office for preventing and combating corruption) and the Money Laundering Prevention Service have SPOCS for centralised domestic cross–agency exchanges. The State Police is implementing the new Criminal Intelligence Model and therefore internal information exchange structures are still to be harmonised for use at all levels and internationally. The International Cooperation Bureau of the State Police is responsible for police exchanges. In Customs the Criminal Investigation Board is responsible for information exchanges with MS, particularly under the Naples II Convention or through the General Prosecutor's Office under MLA procedures. Within the Finance Police Board this is the responsibility of the Information Coordination Dept which forwards requests and replies to the intelligence or investigation Depts as appropriate.

In Lithuania incoming and outgoing international requests for information from/to other EU MS for the purpose of criminal investigations and criminal intelligence operations are co-ordinated and handled by the International Liaison Office of the Lithuanian Criminal Police Bureau. The office implements and co-ordinates the practical co-operation between Lithuanian police and other LEAs and houses the national bureaus of INTERPOL, SIRENE and EUROPOL, liaising with EUROPOL and MS equivalent units. It is also responsible for the implementation of practical co-operation with the police and customs liaison officers, accredited in the Republic of Lithuania. The Customs Criminal Service and Financial Crime Investigation Service (FCIS) is responsible for international co-operation and information sharing between FCIS and appropriate foreign authorities.

In Luxembourg the Police Grand-Ducale is the police force, responsible to the Ministry of Interior. Most of the criminal investigations are conducted by members of the Police, although Customs and certain other Ministries have limited investigation powers. All investigations are done under the supervision of the prosecutors in the two judicial districts of Luxembourg. The International Relations Service of the police (Police Grand-Ducale, Direction Générale, SRI - Service des Relations Internationales) operates as a SPOC for all incoming and outgoing international requests for information.

In Malta the International Relations Unit (IRU) of the Malta Police is the responsible unit for international exchanges. This unit includes within its structure the NCB, ENU and the SIRENE Bureau. It is also the unit responsible for co-ordinating requests for International Co-operation in Police (investigative) and Judicial matters (the latter on behalf of the Attorney General). IRU is a centralized structure within the General Police Headquarters where all specialized investigative units are based. The Customs Coordination Unit evaluates and acts on requests which are within its remit, and the parameters of the Naples II convention. If the information requested or required is beyond the remit of the Customs authority the assistance and co-ordination of the proper authorities is requested, typically in co-operation with the IRU and the specialized investigative units of the police.

In the Netherlands the Department for International Intelligence and Information Exchange (IPOL) is the national central contact point for INTERPOL, EUROPOL and SIS/SIRENE as well as for the national and international liaison officers. The Department is also the central focal point for information exchange on behalf of the Koninklijke Marechaussee (Ministry of Defence) and the platform of Special Investigation Agencies such as the Fiscal Information and Investigation Department (FIOD -Ministry of Finance), Social Information and Investigation Department (SIOD - Ministry of Social Affairs), General Inspection Service (AID - Ministry of Agriculture). Other organizations involved in the international exchange of information are BOOM (Justice) and the Customs (Ministry of Finance). The work of the National Centre for International Legal Aid (LIRC) is also embedded within IPOL. This is a co-operation unit with police staff as well as staff of the National Public Prosecutor Office. Besides the LIRC, there are six regional IRC staffed with members of the police as well as members of the regional Public Prosecution Branch. In relation to incoming requests, LIRC decides on further action and distribution accordingly. In cases where an immediate answer can be provided, based on the checks made in the national databases, an answer is provided by IPOL. In case further handling is needed at regional level, the request is forwarded to one of the six regional IRC centres. Based on a developed channel choice model the LIRC decides for outgoing requests which channel (Interpol, Europol, SIS/SIRENE, the national or the international liaison officers) is the most appropriate to be used. The Customs Service's Customs Information Centre (CIC, also known as DIC) acts as a full 24/7 SPOC for Customs matters as the National Office for Mutual Legal Assistance and Mutual Administrative Assistance. Customs, jointly with its investigation section FIOD, has full investigatory powers and exchanges information extensively with other MS which is reflected in the size of the nationwide Intelligence Department and in extensive direct SPOC to SPOC contacts using Naples II and regulation 515/97 powers and procedures, and to AFIS databases, especially CIS. Customs has several LOs (VERWIJDERD) and there is widespread mutual access to databases. LIRC is seen by Customs as a national P(C)CC.

In Portugal law enforcement is the responsibility of the Ministries of Interior, Justice and Finance: The National Republican Guard (Guarda Nacional Republicana – GNR, mainly in rural areas, highway control and fiscal guard) and Public Security Police (Polícia de Segurança Pública – PSP, civilian force in urban areas), as well as the Immigration and Borders Service (Serviço de Estrangeiros e Fronteiras – SEF), which has a criminal investigation unit and houses the SIRENE office, are under the Ministry of Interior. The Criminal Investigation/Judicial Police (Polícia Judiciária – PJ) under the Ministry of Justice has the mission, under the terms of its organic law and the Organisation of Criminal Investigation Act, to assist the judicial and prosecuting authorities in investigations, to develop and foster preventive, detection and investigative actions, falling within their jurisdiction or the actions which the Polícia Judiciária is entrusted with by the competent judicial and prosecuting authorities. The International Co-operation Unit is part of the Criminal Investigation Assistance Units. The Ministry of Finance is responsible for the Customs and Consumer Tax Directorate (DGAIEC).

In Poland the Police and the separate Border Guard are responsible to the Ministry of Interior and Administration, with the Customs Service (and tax investigation service and tax agencies) responsible to the Finance Ministry. The police is centrally controlled with regional and local units who are respectively overseen by regional and local government. International police exchanges are carried out by the (national) main Police HQ's Division for Coordination of the International Exchange of Information at the Office of International Cooperation of Poland (CIEI OICP). The division houses the bureaux for INTERPOL, EUROPOL and art. 39 and 46 SIS. It is paralleled by the Division of Coordinating International Searches, which co-ordinates the exchange of information in the range of SIS and international searches. These divisions are supported by a 24/7 SPOC manned by, particularly, SIRENE and INTERPOL bureaux staff. Customs has since August 2009 had partial criminal investigative powers and its international exchanges are coordinated centrally at the Department of Customs and Excise Control in the Ministry of Finance. The Border Guard has a similar centre for receiving and exchanging information in its Operations Investigative Board (MHBG). These services and the police have widespread national identification databases (vehicle registrations, identity cards, registers of foreigners, etc.).

In Romania the General Inspectorate of the Romanian police is the lead law enforcement agency under the Interior Ministry. Customs does not have criminal investigative powers but does make administrative exchanges with MS under the Naples II Convention. There is a single national central authority responsible for specialized cooperation activities and international police assistance, the International Police Cooperation Center (IPCC) within the General Inspectorate of the Romanian Police. Its main functions as the national SPOC are related to information exchange in criminal matters, assistance given to the MS liaison officers in Romania, and co-ordination of information exchanges within Romania in relation to international requests. The police and especially the Border Police support this centralized system through 6 PCCs, subordinated to the General Inspectorate of the Romanian Border Police (one with Bulgaria will soon include Customs). Information flows (incoming and outgoing) are shared on local/regional/central level through the e-Cooperate system which is designed to eliminate duplications and is accessible in real time by all relevant agencies. The Romanian Immigration Office coordinates all international exchanges in relation to migration issues through its Central Bureau for Intelligence Analysis Unit, but relevant exchanges are made exclusively through the IPCC.

In Slovakia all police forces and police agencies are incorporated into the Police Presidium which is responsible to the Ministry of the Interior. The Customs Office is responsible to the Finance Ministry. The police are organized centrally with regional and local units. The police coordinating unit responsible for dealing with international exchanges is the International Police Cooperation Bureau (IPCB) which acts as a SPOC working alongside the Schengen Cooperation Bureau. The IPCB deals with the co-ordination of case handling carried out by police bureaux which are particularly involved in fighting international crimes. These are the Judicial and Criminal Police, the Organized Crime Bureau, the Financial Intelligence Unit, the

Railroad Police and the National Immigration Unit of the Border and Alien Police. The Customs Office also has a Liaison Officer at the IPCB as well as having its own International Customs Cooperation Bureau (ICCB). Cross-border co-operation with neighbouring states is ensured through the medium of mutual contact points, which are placed at the borders and act as P(C)CCs ensuring co-ordination of information and its proper notification to the centre.

In Slovenia, the Section for International Police Co-operation (SIPC) within the Criminal Police Directorate is responsible for co-ordinating incoming and outgoing requests through the communication channels for international police co-operation (INTERPOL, EUROPOL, SIRENE, SECI, Liaison Officers, bilateral co-operation) and Customs has an access to all these communication channels. The incoming requests are divided among three units: INTERPOL, EUROPOL and SIRENE, depending on the nature of a request. If there is a request which can be solved by these units they respond and prepare answers. In cases where a request is more substantial, it is sent to an authorized department at central or regional level which then prepares an answer. The Customs Service does not have investigatory powers. Criminal investigations are carried out by the police, but based on data and intelligence supplied by Customs who have a liaison officer with SIPC, and staff units who work closely with SIPC on a regular basis. There is however considerable exchange of intelligence information on Customs matters (and indirectly on tax matters) through input into OLAF's CIS and other AFIS systems.

In Spain the Spanish Constitution gives considerable powers to the Provincial Governments and their autonomous police forces. At national level the Ministry of the Interior is responsible for the Cuerpo Nacional de Policia (the National Police) and the Guardia Civil. At the Provincial level the autonomous police forces are responsible to the Provincial and municipal governments. There are Regional Police Cooperation Centres where the autonomous forces exchange information with the National Police and the Guardia Civil as well as the Judicial Police, with agreements having been made between the Interior Ministry and the Federation of Municipalities and Provinces regarding exchanges between, and access to, investigation and intelligence databases. National information co-ordination is based upon co-operation between the Regions and Municipalities and the Central Unit for Criminal Intelligence in the National Police, and the Central Unit for Analysis of Delinquency in the Guardia Civil (it being a technical unit of the Judicial Police). There is also a Centre of Intelligence against Organised Crime (CICO) which amongst other duties is charged with the co-ordination of activities of the different police organisations (nationally and regionally) in relation to organised crime activities, which involves significant international exchange activity. The International Police Cooperation Unit is the centre for the NCB, ENU, and the SIRENE Bureau. All these central organisations work closely with each other and with the National Centre of Anti-Terrorism Coordination.

In Sweden the Department of Justice oversees the work of the police (Swedish National Police Board – SNPB) including the National Criminal Police and the Security Police, the Prosecution authorities and Swedish Economic Crime Authority. The Coastguard is overseen by the Defence Department, and Customs (and the Swedish Tax Agency) by the Finance Department. The main SPOC (and the national SPOC for police authorities) for international information exchanges is the Unit for International Co-operation (IPO) at the National Criminal Police. IPO is an integrated office, with the three police co-operation channels (SIS/SIRENE, EUROPOL and INTERPOL) being located in the same unit. The contact point secures that all cases are co-ordinated, handled according to the law, securing quality and speed by usage of suitable international channels. The Coastguard has a Liaison Officer at IPO with Customs, the Economic Crime Authority and the Tax Office being located in the Criminal Police Force's Criminal Investigation Service which works closely with IPO. The Tax Office also has a Liaison Officer at the Finance Police. All agencies cooperate within Sweden through Regional Intelligence Centres which have multi agency staffs (including Customs). Customs itself has a new National Coordination Centre (NCC) which is the 24/7 SPOC for information exchanges. Mutual Assistance requests are dealt with by Customs IMAO - International Mutual Assistance Office. All of these Customs units have appropriate access to a single national Customs investigation and intelligence database. Swedish law enforcement agencies make extensive use of the Nordic Liaison Officer Network.

In the United Kingdom (UK) the Serious and Organized Crime Agency (SOCA) is the leading operational authority which routes incoming requests to national agencies and co-operates with EUROPOL and INTERPOL, co-operating with the Scottish Crime and Drugs Enforcement Agency – SCDEA – for Scottish matters and the Police Service of Northern Ireland – PSNI- in Northern Ireland. National agencies within the UK (Scottish Crime and Drugs Enforcement Agency – SCDEA, Police Service of Northern Ireland – PSNI, HM Revenue and Customs – HMRC, and United Kingdom Border Agency - UK BA) have their own International Mutual Assistance Teams (IMATS) responsible for international exchanges, and their own 24/7 Single Points of Contact. IMATs liaise with the United Kingdom Central Authority (UK CA) Judicial Co-operation Unit in the Home Office regarding Mutual Administrative Assistance (MAA) and Mutual Legal Assistance (MLA). UK CA maintains a central register with incoming requests being approved by it and with outgoing requests being sent by it. Regional ("territorial") police forces can and do make non judicial requests directly to other MS. There is close "database co-ordination" between SOCA, SCDEA, UK BA and HMRC, and between these agencies – especially SOCA - and territorial police forces. The already considerable integration of existing investigation and intelligence databases will be enhanced with the introduction of more inclusive ones, such as the PND (Police National Database) to be introduced by late 2010, which will hold intelligence information available to all UK regional forces. SOCA acts on international exchanges in its own right and as the bureau responsible for exchanging information on behalf of regional forces and for liaising with HMRC and UK BA.

3.2 Legal bases

The EU Member States exchange information and criminal intelligence based on EU legal instruments and different bilateral/multilateral agreements, usually regulating exchange of information and criminal intelligence as just one part of a wider cross-border co-operative initiative. The latter were captured by the European Commission in their questionnaire related to legislation (Map 1) and will not be looked at in detail in this Study.

Primary sources of the EU law are the EU's treaties. One of the main treaties is the Treaty on the Functioning of the European Union which includes provisions on police co-operation (art. 87.1) and information exchange (art. 88.2).

The Lisbon Treaty establishes police co-operation involving all the Member States' competent authorities, including police, customs and other specialised law enforcement services concerned with the prevention, detection and investigation of criminal offences. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures concerning:

- the collection, storage, processing, analysis and exchange of relevant information;
- support for the training of staff, and co-operation on the exchange of staff, on equipment and on research into crime-detection;
- common investigative techniques used in the detection of serious forms of organised crime.

Over the past years, numerous legal acts and communication channels have led to a wide choice and created an extensive toolbox for collecting, processing and sharing information between national authorities and other European players in the area of justice, freedom and security. However, the use of a variety of legal bases and communication channels sometimes leads to confusion by making available several appropriate communication channels.

Listed below, and detailed further in the Annex to this study, are the main legal instruments regulating information systems, databases, communication networks, and information exchange for the purpose of criminal investigations and criminal intelligence operations on the EU level:

- Swedish Initiative
- Prüm Decision
- EUROPOL
- Schengen Information System and SIRENE Information Exchange
- Customs Information System (CIS) Convention 1995 leading to the establishment of:
- Anti Fraud Information System (AFIS), both now receiving input by the MAB (Mutual Assistance Broker System from June 2010)
- FRONTEX
- Fado

The EU information systems usually consist of databases and communication networks in accordance with the relevant legal basis and resulting in communication channels being used for cross-border information exchange within the EU. In contrast, the Swedish Initiative and the Prüm Decision are declarations of intent which require implementation through the focused use of existing generic or dedicated databases and IT networks. As they are the focus of this study, the Principle of Availability, the Swedish Initiative and the Prüm Decision will be discussed in more detail below.

Next to the above, the Commission Communication Overview of information management in the area of freedom, security and justice[7] presents the following legal instruments or legislative initiatives[8] (regulations, directives, decisions, treaties, etc) dealing with collection, storage and exchange of data for law enforcement or migration purposes which create the legal basis either for new IT networks or for strengthening the information exchange and law enforcement cooperation among EU MS:

[7] Communication from the Commission to the European Parliament and the Council; Overview of information management in the area of freedom, security and justice, Brussels, 20.7.2010 COM(2010)385 final

[8] Initiatives are listed in italics

- Visa Information System
- Eurodac
- Advanced Passenger Information Directive
- Data Retention Directive
- European Criminal Records Information System (ECRIS) Decision
- Financial Investigation Units Decision
- Cyber Alert Platforms
- Asset Recovery Offices
- Eurojust
- Passengers Name Records Decision
- Terrorist Finance Tracking Programme
- Entry/Exit system
- Registered Travellers Program,
- Electronic System of Travel Authorisation (ESTA)
- European Police Records Information System (EPRIS)

In addition to EU level instruments there are also many relevant bilateral agreements which either include information exchange or indeed have a focus on cross-border information exchange, specifically those establishing and regulating

- Liaison officers network,
- Police and Customs Co-operation Centres

INTERPOL is included in this legal overview, although INTERPOL is not a part of the EU legal framework, as it has a very significant role in the cross-border information exchange within the EU.

Table 2: Overview of the main legal documents related to information exchange for the purpose of criminal investigations and criminal intelligence operations in the pre-trial phase in the EU

	Objectives	Legal Basis
SWEDISH INITIATIVE	More effectively and expeditiously exchange existing information and intelligence for the purpose of conducting criminal investigations or criminal intelligence operations	Framework Decision 2006/960 JHA on simplifying the exchange of information and intelligence between LEA of the EU MS
PRÜM DECISION	Step up cross-border co-operation and exchange of information between authorities responsible for the prevention and investigation of criminal offences (no collection, storing and supply of personal data)	-Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime -Council Decision 2008/616/JHA on the implementation of the -Council Decision 2008/615/JHA
EUROPOL	Support and strengthen action of the MS in combating organised crime and other forms of serious crime, affecting at least two MS	Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (replaces the provisions of the EUROPOL Convention)
INTERPOL	Facilitation of international police co-operation and the enabling of police in all its member countries to request, submit and access vital data instantly in a secure environment	-INTERPOL Constitution and General Rules -Implementing rules for the rules on the processing of information for the purposes of international police co-operation -International agreements with states and other organizations
SCHENGEN SIS	Maintain public order and security, including border control, state security, and to apply the provisions of the Schengen Convention relating to the movement of persons (article 93)	-Convention implementing the Schengen Agreement of 14 June 1985 -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) -Council Decision 2007/533/JHA of 12 June 2007 on establishment, operation and use of the second generation SIS (SIS II) -Commission Decision adopting SIRENE Manual, 4 March 2008
CUSTOMS INFORMATION SYSTEM (CIS)	Assist in preventing, investigating and prosecuting serious contraventions which are in breach of Community Customs or Agricultural legislation or which constitute serious infringements of National law in these or related areas	-Convention on the use of information technology for customs purposes (CIS Convention-95) -Council Regulation (EC) No 515/97 of 13/3-97 on mutual assistance between the administrative authorities of the MS, as amended -Council Regulation (EC) No 766/2008 of 9/7-2008 amending Regulation (EC) No 515/97 -Convention on mutual assistance and co-operation between customs administrations (Naples II Convention) of 1997, the equivalent instrument for prosecution of offences against Community Law in the Customs sphere, which is the current basis for exchange of information to prevent and detect violations of national Customs legislation, i.e. Third Pillar matters, and for prosecutions in relation to EC interests, i.e. First Pillar matters
ANTI FRAUD INFORMATION SYSTEM (AFIS)/MAB	Exchange of anti-fraud information between OLAF and competent administrations for investigation and intelligence purposes	-Council Regulation (EC) No 515/97 of 13/3-97 on mutual assistance between the administrative authorities of the MS Council -Regulation (EC) No 766/2008 of 9/7-2008 amending Regulation (EC) No 515/97 -Regulations 595/91, 1681/94 1831/94, 2584/00,44/2003 -Mutual assistance agreements with third countries -CIS Convention -Naples II Convention
FRONTEX	To co-ordinate operational co-operation between Member States in the field of management of external borders and carry out risk analyses	-Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Co-operation at the external Borders of the MS of the EU
FADO	To exchange information which the MS possess concerning genuine and false documents that have been recorded	Joint Action (98/700/JHA) of 3/12-1998 adopted by the Council on the basis of Article K.3 of the Treaty on EU concerning the setting up of a European Image Archiving System (FADO)
LIAISON OFFICERS	Further accelerate co-operation by providing assistance in the form of the exchange of information for the purposes	Bilateral/Multilateral agreements between MS

	of combating crime and (article 47 SC)	
P(C)CCs	To assist each other for the purposes of preventing and detecting criminal offences (article 39/4 Schengen Convention)	- 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 Article 39/4 - Bilateral/ Multilateral Agreements

3.2.1 Principle of Availability

The Principle of Availability (PoA) means that, throughout the EU, a law enforcement officer in one Member State who needs information in order to perform his duties should be able to obtain this from another Member State, and that the law enforcement agency in the Member State that holds this information will make it available for the stated purpose, taking into account the requirements of any ongoing investigation in that State. The EU launched several initiatives in order to improve the effectiveness of information and criminal intelligence exchange with EU and the principle of availability is a key issue in the third pillar co-operation. The PoA can therefore be said to be a cornerstone and a vision for law enforcement co-operation. A first step to implement the PoA, representing the classic "police-to-police approach", i.e. indirect access to information upon request, was taken on 18th December 2006 by adoption of the Framework Decision on simplifying the exchange of information between the LEAs in the EU; a total of 49 types of relevant information were identified together with each Member State's legal potential to make them available. The implementation of the PoA can also be recognized when Rapid Intervention Teams are deployed in an EU Member State facing a mass influx of third country nationals attempting to enter EU territory illegally. In these cases the host EU Member State may authorise the members of the Rapid Intervention Teams, consisting of EU MS border guards, to consult its national and European databases, which are necessary for border checks and surveillance[9]. The incorporation of the Prüm Treaty into the EU acquis is the most concrete example regarding the PoA, though it is not the only one. There are several other instruments which give Member States instant access to relevant information (EUROPOL Information System, SIS, FIND – Fixed INTERPOL Network Database, MIND – Mobile INTERPOL Network Database, etc.), based on the Principle of Availability.

Both EUROPOL and INTERPOL expressed a clear need for MS to significantly increase their inputs to these systems, though MS have made progress in this respect. The reality is that the scale of spontaneous information and intelligence exchange through these information systems, which can be seen as an intermediary between "information and intelligence providers" and "information and intelligence seekers", is not on a high level and much more should be done in this area in the future. Several MS (e.g. France, Finland), as well as INTERPOL and EUROPOL, have highlighted the need to overcome this lack of pro-active sharing of information which might potentially be important for law enforcement authorities in other MS. In the Customs

[9] The members of the teams shall consult only those data which are required for performing their tasks and exercising their powers. The host Member State shall, in advance of the deployment of the teams, inform the FRONTEX of the national and European databases which may be consulted. The Agency shall make this information available to all Member States participating in the deployment; REGULATION (EC) No 863/2007 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 July 2007 establishing a mechanism for the creation of Rapid Border Intervention Teams and amending Council Regulation (EC) No 2007/2004 as regards that mechanism and regulating the tasks and powers of guest officers

sector MS and OLAF pointed out that the Customs Information System (CIS), a long established EU wide system for MS to input intelligence for use by other MS, did not have nearly as much information as might be expected. It is hoped that the new MAB system, which is easier to operate, will improve the situation significantly, but the primary factor is the motivation to give information which may be of use to others.

The implementation of the PoA is a complex issue which affects the home affairs of each Member State, as well as the legal, technical and operational capabilities of the MS. The PoA is a goal impossible to reach, due to differing national systems and capabilities (both regarding interoperability of retrieval and exchange systems, and the actual availability of information). At the same time, some Member States have been applying the principle - for over 10 years. If available and legally capable of disclosure, information will be made available. However, when a Rogatory Letter is required the PoA is not being used and in these cases cross-border information exchange is usually slowed down, often significantly.

The aim of expanding the scope of application of the PoA should be stressed. As a rule information received from other MS through existing information exchange channels may not be used as evidence during judicial procedures. The Lisbon Treaty, Hague Programme, Swedish Initiative, Prüm Decision and other acts of law legally grounding information exchange between MS LEAs underline the main purpose of information exchange and LEA co-operation - to detect, prevent and investigate crimes and criminal activity. Crime investigation also includes LEA activities aimed at the collection of admissible evidence to be used during judicial procedures. The current level of implementation of the PoA supports the operative LEA activities but has no actual influence on activities regulated by the norms of criminal laws when collecting evidence. During activities related to judicial proceedings, formal procedures of information acquisition through Rogatory Letters, mutual assistance procedures, etc. are usually required, which hampers operative criminal procedures and fails to serve the needs of justice effectively.

3.2.2 Swedish Initiative

Framework Decision 2006/960 JHA on simplifying the exchange of information and intelligence between LEA of the EU MS foresees that a MS law enforcement agency can only deny access to information to another MS under the circumstances described in Article 10, i.e. that they:

- harm essential national security interests,
- jeopardise the success of a current investigation or a criminal intelligence operation or the safety of individuals;
- are disproportionate/irrelevant with regard to the purposes for which it has been requested
- the respective judicial authority has not authorised such exchange, where needed

If the relevant offence is punishable by imprisonment of one year or less under the law of the requesting Member State, the competent law enforcement authority may also refuse to provide the requested information.

The “Swedish Initiative” not only sought to enshrine the Principle of Availability in law, but also to advance co-operation by setting time limits to answer requests of information. An urgent request should ideally be answered within 8 hours, while other information held in databases readily accessible by the authority should be provided within one week. If the information is not so readily accessible a timeframe of two weeks is given.

The "Swedish Initiative" does not define the term "urgency". However, "urgent" cases can be understood to mean any situation during which the sought for information will:

- prevent a risk of death or harm to persons or serious damage to property;
- result in, or terminate, a decision involving deprivation of liberty (where such a decision has to be taken within a short period of time);
- prevent the loss of information that is important for the further stages of an investigation.

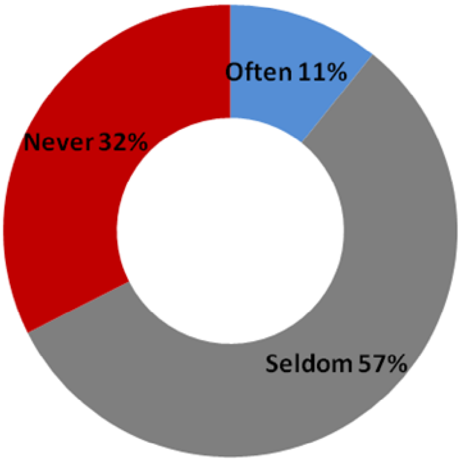
Examples of such situations are:

- abductions and hostage-takings;
- the risk that a serious offence will be committed or repeated;
- the disappearance of minors, and the disappearance of adults giving cause for concern;
- decisions relating to keeping a person in police custody, or remanding a suspect in custody or releasing a person;
- the possible escape of a suspect in a serious case;
- the need to obtain information at risk of imminent destruction[10]

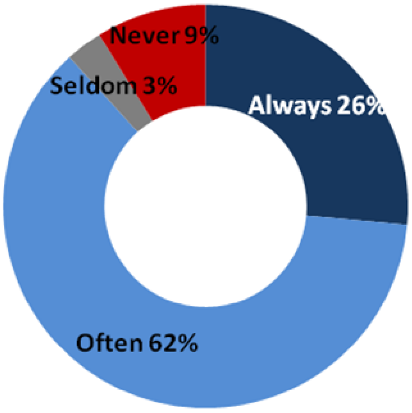
The graphs below indicate that the requests for urgent data transmission are not very often used by MS, but almost 90% of MS say that their EU partners always or often comply with urgent requests. The main reasons for not complying with an urgent request are lack of personnel and unavailability of information at a national level.

[10] 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

Q 26 - Urgent requests. How often do you request urgent data transmission, i.e. within 8 hours?



Q 27- Urgent requests met. In your experience, do EU partners comply with your urgent requests for information or criminal intelligence?



In accordance with Article 6 of the Swedish Initiative[11], Member States may choose any existing communication channels used for international law enforcement co-operation. The most used communication channels for this purpose are the following:

- SIRENE channel
- EUROPOL channel
- INTERPOL channel
- liaison officer's channels
- mutual assistance channels among customs authorities (Naples II)
- bilateral channels

MS decisions on selection of communication channel usually depend on the subject matter, requested country, level of security/confidentiality and urgency of the request. According to the Manual of Good Practices concerning the International Police Co-operation Units at national level[12] the following criteria should be observed while selecting the most appropriate communication channel:

- geographical approach:
    - o nationality/residence/origin of person or object concerned is known and request concerns establishing details (address, phone number, fingerprints, DNA, registration, ...)
    - o nationality/residence/origin of person or object concerned is not known
- thematic approach:
    - o EUROPOL (organised crime, at least 2 MS, connection to AWF, need for joint approach)
    - o confidentiality / sensitivity
    - o channel used for previous related request
- technical approach:
    - o IT-criteria: need of secure channels (BDL for intelligence and terrorism-related
    - o information or technical compatibility (SIRPIT for fingerprints)
- urgency
    - o urgency / proven speed of channel (in particular immediate risk for person's physical integrity, immediate loss of evidence, request for urgent cross-border operation or surveillances)
    - o priority

Requested MS usually respond by using the same communication channel as was used for the incoming request. In cases where a requested MS replies by using another communication channel, the requested MS informs the requesting MS about the communication channel(s) that is going to be used.

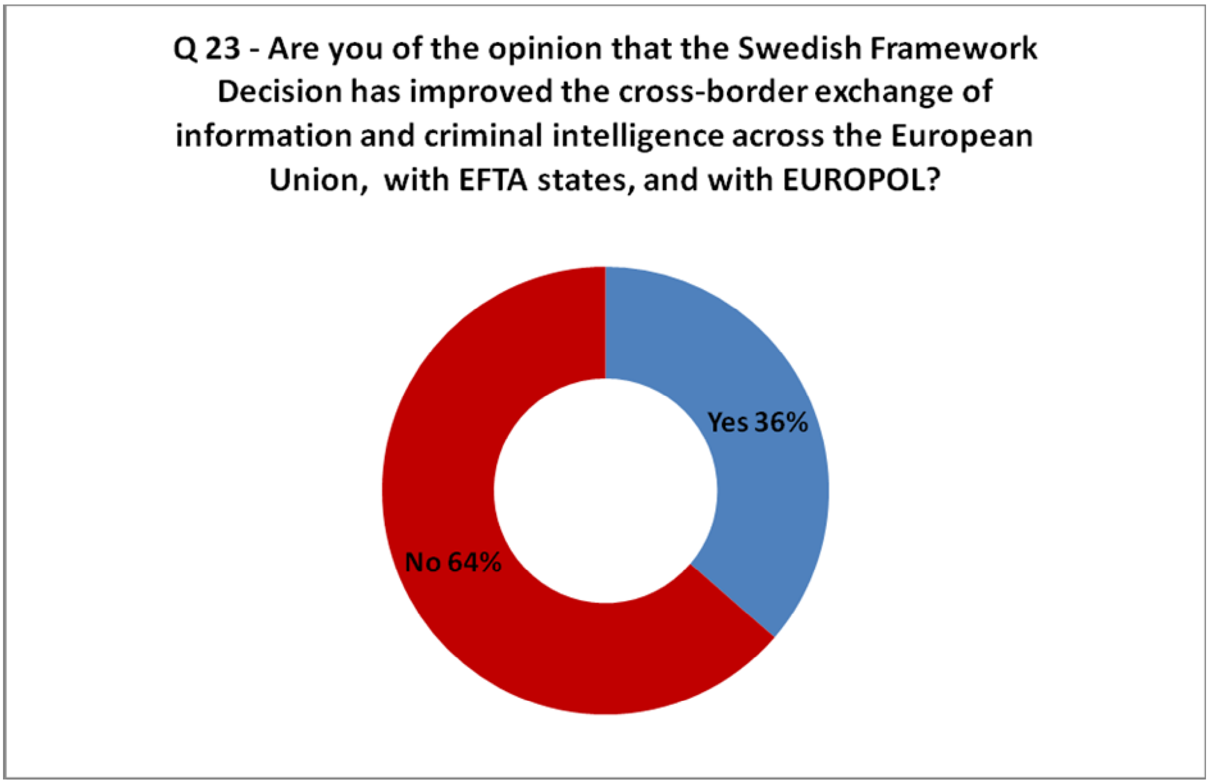
Whenever a request falls within EUROPOL's mandate, the answer provided by the requested Member State should also be copied to EUROPOL. This principle has to be applied whatever the channel chosen, including the EUROPOL channel.

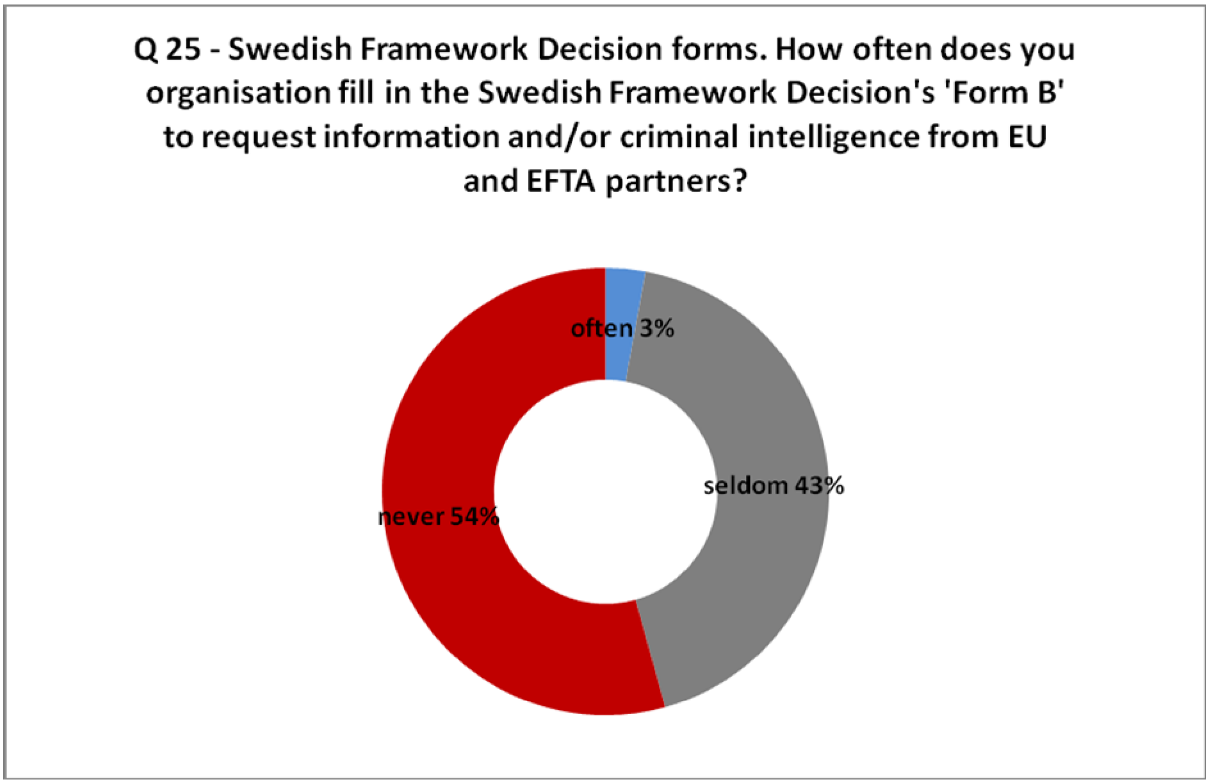
[11] Swedish Initiative (Council Framework Decision2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union)

[12] Document 7968/08 ENFOPOL 63 + COR 1

In this respect a difference has to be made between, on the one hand, the use of the EUROPOL communication channel as a means of information exchange between Member States, using their liaison officers and, on the other hand, the direct communication to EUROPOL, as an organisation, for any intelligence falling within its mandate.

The "Swedish Initiative" was intended to be a major step towards making law enforcement information more easily available throughout the EU. In principle it is a good idea but unfortunately very seldom used by Member States. Only few MS use the content and almost no single MS uses the form which is considered to be rather complex and cumbersome. Where it is used, it is often only by some agencies within a State (e.g. by UK SOCA's Asset Recovery Office (ARO) in relation to complex financial transactions.). Users prefer free text reporting, instead of filling in several pages of modular information, increasing time spent handling the requests. Even the simplified version of form B, developed during the Czech Presidency, has not brought the expected results. The form is typically not used in standard cases of communication because sending information in attachments instead of in the main text of an email means additional work and uses up computer capacity. This latter point was stressed by several MS. Additionally, as mentioned above, there was no agreement on using only a pre-defined secure information channel (e.g. only EUROPOL or any other channel) to exchange information and criminal intelligence, and structured automated data exchange is therefore missing. According to the EU MS, the main benefit of the Swedish Initiative is the determined tight deadline of 8 hours for urgent requests, which has improved the cross-border information exchange procedures in urgent matters. At the same time, also the simple fact that the SI provides a broad legal framework for information exchange can be said to have improved cross-border exchanges. The SI might be used as legal basis more often than it gets credit, as reference might still be made to Arts 39 and 46 of the Schengen Convention while Art 12 of the Swedish Framework Decision largely supersedes these two Articles. This will be the norm as all MS will have brought the Framework Decision within their national legislation.


Q 23 - Are you of the opinion that the Swedish Framework Decision has improved the cross-border exchange of information and criminal intelligence across the European Union, with EFTA states, and with EUROPOL?


Q 25 - Swedish Framework Decision forms. How often does you organisation fill in the Swedish Framework Decision's 'Form B' to request information and/or criminal intelligence from EU and EFTA partners?

Although the number of requests was not encompassed in this Study, the replies provided to the European Commission in 2009[13] clearly confirm the aforementioned findings that the Swedish Initiative is quite rarely used. At the same time it has to be mentioned that it might not be easy

[13] On 27/4/2009 the EC COM convened a meeting to assess the implementation of the Swedish Initiative and presented below figures. Please note that the project team was informed by France that the Swedish Initative had not been transposed in national law by June 2010.

to distinguish which legal basis requests are based upon, and countries might have used different bases for counting. Furthermore, the Framework Decision has not been transposed into national law by all countries yet, or in some countries like Spain this has only very recently been achieved, which is not properly represented in the table below.

Table 3: Requests sent on the basis of the Swedish Initiative[14]

BE	19	MT	0
BG	0	NL	2
CZ	3	AT	0
DK	N/A	PL	0
DE	531 (of which 8 were urgent)	PT	N/A
EE	0	RO	0
IE	5	SI	6
EL	N/A	SK	0
ES	0	FI	0
FR	1,314	SE	40
IT	N/A	UK	0
CY	0	NO	0
LV	4	IS	0
LT	0	CH	N/A
LU	N/A	LI	0
HU	0		

Based on the interviews in the visited MS and on the questionnaire's answers provided by MS, it can be clearly established that the Swedish Initiative has not facilitated the exchange of information within the EU as hoped because the EU MS dislike using the SI form which is, according to the majority of MS, too cumbersome. Even the shortened version, developed under the Czech Presidency, is not often used: EU MS prefer more flexibility through free text rather than using only the prescribed fields of the SI forms. Nevertheless, the Swedish Initiative has brought certain advantages, such as identification of clear and common sets of data categories and strict time limits, even if it is not often used for urgent requests. In addition, while it may not have led to significant changes in practice, the Swedish Framework Decision does provide a legal basis for data exchanges between all EU MS and EFTA countries.

In summary we can conclude that:

[14] As presented by the EC during the Second meeting of the Sub-Group on Police Cooperation Statistics 10 February 2010, Brussels

- The Swedish Initiative provides a legal basis for the exchange with MS and EFTA states as well.
- The Swedish Initiative clearly identifies time limits and categories of information
- The SI forms are too cumbersome for practitioners. Especially in urgent cases it is seen as hindering the requester rather than facilitating prompt action.
- The implementation of the SI is pending in some MS and not persistent in the majority of MS' business work flows.

3.2.3 Prüm treaty

On 27 May 2005, Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria signed in Prüm/Germany the Treaty on the stepping up of cross-border co-operation, particularly in combating terrorism, cross-border crime and illegal migration. Since then Finland, Slovenia, Hungary, Bulgaria, Romania, Slovakia and Estonia have acceded to the Treaty.

The "Prüm" Decision incorporates the main provisions of the 2005 Prüm Treaty into EU law. The Council Decision 2008/615/JHA of 23 June 2008 foresees in Article 36 that all Member States shall take the necessary measures to comply with the provision of the Decision

- for the supply of non-personal and personal data for major events, the supply of information in order to prevent terrorist offences, joint operations and assistance in connection with mass gatherings, disaster and serious accidents by 26 August 2009;
- for the exchange of DNA profiles, dactyloscopic data and vehicle registration data by 26 August 2011.

The scope of the Prüm Treaty was to enhance cross-border law enforcement and judicial co-operation and to increase the exchange of judicial and police information. It provided for the signing Member States access to data bases of the other countries on a HIT/NO-HIT basis – similar to the global system operated by INTERPOL - and, secondly, within the scope of mutual assistance, to request and exchange personal data.

The Prüm Decision enables law enforcement authorities to exchange information across borders by using the following tools:

- Automated searching for DNA-profiles
- Automated searching for dactyloscopic data by use of mutually accessible technical entry to their "automated fingerprint identification systems" (AFIS)
- Automated searching for vehicle registration data in the European Vehicle and Driving License Information System "EUCARIS"
- Police Co-operation

In other words, a law enforcement officer in one MS can see if DNA material (or fingerprints) obtained during the investigation has a "match", not only in the national system, but also in the corresponding national systems of other EU MS. Automated inquiries can be sent selectively by choosing one, several or all of those EU MS who are legally and technically ready to process Prüm requests. However, the officer does not have direct access to information on personal details or case details of the HIT case. This information still has to be requested separately, through mutual assistance, and in particular by applying the rules and the Principle of Availability. Legal assistance procedures start after a match is obtained during the automated consultation phase and after validation of a match by the requesting party.

In contrast to the Swedish Initiative, the Prüm Decision seems to be one of the most efficient tools to identify criminals and solve crimes, based on biometric data. According to those MS where the decision has been fully implemented, the possibility of almost instantly knowing if a certain type of information is available in another MS and where, without any formal request, is regarded as enormous value to investigations, gaining time and increasing efficiency, and many EU MS stressed that further development of information and criminal intelligence sharing should follow HIT/NO-HIT systems.

By November 2009, the Treaty was in force in 14 Member States of the European Union. By the end of 2009, 10 EU MS were operational in exchanging DNA data, whereas only 5 MS - only partly overlapping with the countries exchanging DNA data - were using the automated fingerprint exchange, 8 MS exchanging DNA. No MS indicated any serious problems complying with Chapter 2 of the Prüm Decision concerning the automated exchange of DNA, fingerprints and vehicle registration data. Technical problems have been mainly confined to technical incompatibilities which have led to difficulties in interfacing between different national fingerprint databases.

Difficulties arise mostly at the stage of follow-up requests. The different legal and procedural regimes differentiating between information obtained by police and by judicial authorities present problems. For the same type of information (e.g. DNA), and depending on the country, MS can ask for nominal information through police co-operation channels if in the destination country it is considered a police issue, while in other countries it may be considered judicial information to be exchanged only through a request for mutual assistance. The selection of the communication channel for the exchange of supplementary data varies from country to country. Some Member States use the INTERPOL channel (e.g. Austria, Slovenia, Germany) while others use EUROPOL (e.g. France).

3.3 Scale of cross-border information exchange

Cross-border information exchange has significantly increased in almost all EU MS over the last few years. The main reasons for this include enlargement of the Schengen area, newly concluded bilateral or multilateral agreements on police and customs co-operation and exchange of information, direct bilateral liaison, the enhanced role of joint investigation teams, the efficient work of Police and Customs Co-operation Centres, greater knowledge and awareness of cross-border information exchange, improved and strengthened exchange capabilities, increased effectiveness of exchanges, etc. Clearly, too, the levels of international organised crime have had an impact on the scale of cross-border information exchange, and on the type of data exchanged.

One of the findings of this Study reveals that the majority of information and criminal intelligence is exchanged between neighbouring countries. However, there are some exceptions, because the exchange of information also depends on cultural and economic links, the criminals themselves, and the nature of the crime. For example, information exchanges between France and Spain place a very high priority on cases relating to counter terrorism against ETA with relatively high volumes of such counter terrorism exchanges. While such cases are obviously top priority in all MS, numbers of such exchanges are typically much smaller in some other MS. High volumes of top priority cases between France and Italy, Greece and Malta are, for instance, related to illegal immigration. However, this factor of exchange between neighbours should not be overstressed, as cross-border crime increases not only between neighbour states but also between states geographically more distant from each other.

The scale of cross-border information exchange also depends on the authority's specialization, the nature of the criminal activities and the scope of work responsibilities. For example, if there is an authority only dealing with illegal immigration (e.g. Border Guard, Immigration Service) or has only a few responsibilities, but they include illegal drugs (Customs), its work is mainly connected to cross-border exchanges and the scale of cross-border information exchange is usually fairly high. In contrast, a much lower scale of cross-border exchange occurs when a more general authority (crime police) is dealing with different kinds of domestic and foreign crimes. Moreover, the scale of cross-border exchange is usually higher in border areas and for this reason it is impossible to define the exact scale of cross-border information exchange, even in one single MS.

According to INTERPOL, approximately 13,000,000 messages were exchanged in 2009 worldwide and approximately 2,000,000 were exchanged among EUROPOL and the EU MS[15]. Although these numbers are not directly comparable, the figures show quite a significant importance for the INTERPOL channel for cross-border exchanges within the EU.

[15] Data provided by INTERPOL

The tables below indicate an approximate level of internationalization of the LEA's work[16]. From the data, provided by EU MS, it can be established that in approximately ¼ of investigations and criminal intelligence operations requests are send to other EU or EFTA MS. In addition, MS provide answers to other MS in almost all cases.

The category of denied information is almost non-existent. Member States usually explain the reasons that hinder the provision of certain information or criminal intelligence, and when an explanation is given this cannot and indeed is not treated as a denial of information or criminal intelligence. MS are very often not permitted to provide IP addresses, domain owners, data of users or owners of payment cards, subscribers of telephone numbers, or financial data such as the existence of, or details within, bank accounts and money transfers, and information held by banks, financial institutions and insurance companies on balances or transactions, etc. due to the national data protection legislation. Such information would usually require Judicial Authorization for disclosure. However, very rarely there are cases when MS do not respond at all, but, according to the MS, this cannot be treated as a denial of information or of criminal intelligence.

Outgoing requests

Table 4: Outgoing Requests – Police Authorities

MS	Police Authorities[17]	Portion of investigations and intelligence operations where requests were sent to other EUMS or EFTA LEA's
BG	International Operational Police Coop. Directorate (ENU)	In roughly ¾ of investigations or intelligence operations
CY	National Central INTERPOL Bureau	2006- 224, 207-345, 2008-358, 2009 -290
DK	National Centre for Investigation	In roughly ¼ of investigations or intelligence operations
FI	National Bureau for Investigation	In roughly ¼ of investigations or intelligence operations
HU	International Law Enforcement Co-operation Centre	In roughly ¼ of investigations or intelligence operations
LV	Latvian State Police	In roughly ¼ of investigations or intelligence operations
LT	National Unit of INTERPOL	In roughly ¾ of criminal investigations or intelligence
LU	Police Grand Ducale, SRI – Service des Relations Internationales	In roughly ¾ of criminal investigations or intelligence
MT	Malta Police – International Relations Unit	In roughly ¼ of investigations or intelligence operations
PL	Office of International Co-operation of Poland, Division of Co-ordination of International Exchange of Information	Very often, in roughly 3/4 of investigations or intelligence operations
RO	General Inspectorate of Romanian Police	In roughly ¼ of investigations or intelligence operations
SK	Presidium of Police Force	10%
SI	General Police Directorate	18.000

[16] The tables include only those MS's answers where data were provided or estimations were made in the questionnaire. Some important qualifying comments need to be made regarding the replies given by police and customs services: A number of absolute figures or, more often, percentage figures, from some agencies are very different from the ranges given by the majority of replying agencies and MS as a whole. These may be transcription errors, due to translation problems, or very possibly misunderstandings of the nature of the requests. Additionally, replies indicating significantly differing proportions may well reflect the role of the responding agency, e.g. where the agency is exclusively involved in cross-border exchanges the proportions will obviously be very high. Where international exchanges are only part of the agency's responsibilities, the proportion is, not surprisingly lower. Equally, the size of the country will have an impact on the proportion of international exchanges. The Project has concluded that, given the consistency of the ranges of statistics given by most agencies in most MS, the conclusions reached remain entirely valid.

Table 5: Outgoing Requests - Customs Authorities

	Customs Authorities	Portion of investigations and intelligence operations where requests were sent to other EUMS or EFTA LEA's
AT	Enforcement and Anti fraud Unit in the area of Taxes and Customs (MoF)	In roughly ¾ of all investigation or intelligence operations
BG	Customs Agency	4 cases in 2009
CY	Department of Customs and Excise	In nearly all investigations or intelligence operations
CZ	General Directorate of Customs	In roughly ¼ of investigations or intelligence operations
EE	Tax and Customs Board, Investigation Department	In roughly ¼ of investigations or intelligence operations
FI	National Board of Customs, Enforcement Division, Intelligence and Investigation	In roughly ¼ of investigations or intelligence operations
HU	Customs	5-10%
IE	Revenue Commissioners, Investigations & Prosecutions Division, Customs Investigation and Customs Drug Law Enforcement	In roughly ¾ of investigations or intelligence operations
LV	Customs Criminal Investigation Board of the State Revenue Service	In roughly ¼ of investigations or intelligence operations
LT	Customs Criminal Service, International Relation Division	50%
MT	Customs	1%
SE	Customs	15%

Incoming requests answered

Table 6: Requests Answered - Police Authorities

Member State	Police Authorities	Portion of investigations and intelligence operations where MS provide information or intelligence to other EUMS or EFTA LEA's upon request
AT	Criminal Intelligence Service, Project Team/International Department	90% (detailed classification is not available, thus the exact number of incoming request cannot be defined)
BG	International Operational Police Coop. Directorate(ENU)	In nearly all investigations or intelligence operations
CY	National Central INTERPOL Bureau	2006- 651, 207-701, 2008-633, 2009 -735
DK	National Centre for Investigation	In nearly all investigations or intelligence operations
FI	National Bureau for Investigation	In nearly all investigations or intelligence operations
HU	International Law Enforcement Cooperation Centre	In nearly all investigations or intelligence operations
IE	Irish Police Service	Provide in excess of 90% of information requested
IT	Joint answer	In almost all criminal investigations or intelligence operations
LV	Latvian State Police	Almost 100%; in nearly all investigations or intelligence operations
LT	National Unit of INTERPOL	In roughly ¾ of criminal investigations or intelligence
LU	Police Grand Ducale, SRI – Service des Relations Internationales	In roughly ¾ of criminal investigations or intelligence
MT	Malta Police – International Relations Unit	In roughly 3/4 of investigations or intelligence operations
RO	General Inspectorate of Romanian Police	In nearly all investigations or intelligence operations
SK	Presidium of Police Force	Approximately 10%
SI	General Police Directorate	58.000
UK	Kent Police, Great Manchester Police	Nearly all requests; It is estimated that more than 85% were successfully returned (in nearly all investigations or intelligence operations

Table 7: Requests Answered - Customs Authorities

Member State	Customs Authorities	Portion of investigations and intelligence operations where MS provide information or intelligence to other EUMS or EFTA LEA's upon request
AT	Enforcement and Anti fraud Unit in the area of Taxes and Customs (MoF)	In roughly ¾ of all investigation or intelligence operations
BG	Customs Agency	14 cases in 2009 within the framework of NAPLES II; in nearly all investigations or intelligence operations

CY	Department of Customs and Excise	In nearly all investigations or intelligence operations
CZ	General Directorate of Customs	In nearly all investigations or intelligence operations
EE	Tax and Customs Board, Investigation Department	In nearly all investigations or intelligence operations
FI	National Board of Customs, Enforcement Division, Intelligence and Investigation	In nearly all investigations or intelligence operations
HU	Customs	0.04%
IE	Revenue Commissioners, Investigations & Prosecutions Division, Customs Investigation and Customs Drug Law Enforcement	In roughly ¾ of investigations or intelligence operations
LV	Customs Criminal Investigation Board of the State Revenue Service	Almost 100%; in nearly all investigations or intelligence operations
LT	Customs Criminal Service, International Relation Division	183 incoming requests during 2009
MT	Customs	1%
SK	Slovak Customs Office	Approximately ¼ all cases
SE	Customs	In nearly all investigations or intelligence operations

In the course of the Study, Member States could not provide exact answers to the statistical questions related to incoming and outgoing requests due to the lack of (comparable) statistics available. Member States usually have statistics on crime, but it is much harder to estimate the percentage of crimes that require international co-operation, and national statistical methods and categories of statistical data also differ from MS to MS. For this reason it is almost impossible to compare the data and therefore to identify levels of internationalization of police work and the scale of cross-border information exchange, without the prior existence of common parameters and indicators. However, there are some rough estimates, varying from country to country, which may give an approximate answer regarding the level of internationalization of the country's LEAs' work, or the scale of cross-border information exchange. Moreover, there are also significant volumes of exchange which are not being included in the statistics, e.g. between the Nordic countries, P(C)CCs, and within the framework of Joint Investigation Teams.

Improved statistics would be of great value. They would, for instance, enable early identification to be made on an EU wide basis of the relative resource loadings being placed on MS when carrying out resource intensive work on behalf of other MS, most obviously in relation to the EAW and EIO. They would also help to identify more easily the relative effectiveness of databases and the resulting working methods where such effectiveness depends, to considerable extents, on voluntary pro-activity from MS (e.g. EUROPOL and OLAF intelligence databases).

The creation of central "administrative registers" or "logbooks" of information exchanges covering all relevant agencies in a MS could address this lack of (comparable) statistics. Such central registers or in those of individual agencies, could keep simple records of the details of exchanges and their categories (automated systems, which could be used/adapted exist to an extent as registration is required for data protection compliance purposes). Such systems should be standardised across MS, with common definitions of categories of exchange, and recording guidelines. These should reflect, amongst others matters, that a request can be simple and responded to with only one consultation of a register, or it can require multiple actions and time consuming consultations with other agencies, resulting in a great deal of work (see also next chapter). This latter category of complex requests could thus be "weighted" to reflect the involvement of follow-up requests/actions.

3.4 Types of information

The scale and type of the exchange of data may vary according to an institution's scope of work and its responsibilities. Customs authorities may more often exchange financial data, while police authorities may more often exchange information and criminal intelligence on persons and vehicles. Moreover, national authorities usually exchange all types of data while information and intelligence shared through P(C)CCs is likely to be of a very particular kind. Nevertheless, the answers provided by MS reveal that the following categories of data are very often exchanged:

- Data about persons; perpetrators, suspects, unidentified persons (name, date of birth, jobs, identification data of fingerprinted criminals for true identification, confirmation of identity, residence, DNA, fingerprints, verification of personal data, criminal convictions, passports, IDs, photographs)
- Data about vehicles; vehicles used to transport suspects, perpetrators; vehicles located at the crime scene or recorded by surveillance cameras, registration details, owner and operator of a vehicle, chassis numbers, purchase documents, export and import documents
- Financial data; company information, banking information, property relationship, bank accounts, transaction details, account holders, company board of directors, share capital, income and wealth information, unusual or suspicious money transactions, asset tracing data payment cards, data for POS terminal devices
- Communication data; subscribers' details (particularly for mobiles), IT addresses, billing details, outgoing/incoming calls, emails, wiretapping, interceptions

Data about objects confiscated objects, objects related to committed crimes are often exchanged while data about firearms (licensing data, lost weapon, weapon used for crimes) and other "explanatory" data are seldom exchanged (e.g. interrogations, home searches, seizure of evidence, trends, statistics, customs documents, modus operandi, and fines).

From a general point of view, at the EU level law enforcement agencies have not noticed significant increases or decreases in numbers of requests of any particular type of information or notifications of particular crimes. The fact is that increases or decreases may vary from country to country in relation to national or regional trends in crime and to domestic priorities where the Police put more emphasis on a particular type of crime; in these cases there can consequently be an increase in particular types of request.

Nevertheless, some MS indicated increases of particular types of information or criminal intelligence in the following areas, which, it will be noted, include a number of high impact crimes which are resource intensive from an intelligence and investigation perspective:

- IT related requests in all areas of crime (e.g. theft and fraud, child pornography, money laundering, etc)
- electronic fraud (credit card skimming)
- counterfeited money
- drugs trafficking
- large scale smuggling and counterfeiting of cigarettes and other excise goods

- trafficking of human beings, both for illegal working and for sexual exploitation
- international terrorism
- DNA checks, since the Prüm treaty has been implemented in several MS (increased need for information exchange in HIT cases)

Significant increases have been noticed especially in Bulgaria where trafficking of human beings requests doubled or even tripled in relation to the EUROPOL AWF PHOENIX, as well as follow-up requests related to this AWF. Generally speaking, it is highly likely that the number of international requests will increase more in the future due to greater cross-border mobility in MS as it becomes easier to work in, as well as to visit, other MS. Decreases were only noticed when new MS joined the EU in cases of refusals of entry, and of the supplementary data related to these alerts.

However, different attitudes to crimes, different priorities and different definitions of crimes also have an impact on the levels of cross-border information exchanges and sometimes present practical problems. For example, in some countries, the smuggling of 500g of cocaine - such as in the case study - is a serious crime requiring cross-border co-operation and information exchange, while in others this would not be considered significant. Cattle theft may be of significant importance in one country but not so in others. It should also be noted that some acts might constitute criminal activity in some countries but be quite legal in others.

The threshold of approximately UK£ 3000, reported by some MS as a financial impact value below which the UK may typically not take a EUROPOL or INTERPOL enquiry has, for some MS, presented an obstacle as some severe crimes may not necessarily have a “financial impact” at or above this level. However, the UK Crown Prosecution Service has confirmed that there is no formal limit. ICPO London have an informal limit at this level, but point out it relates to "one off requests" and would not apply to cases with wider ramifications. The UK has however pointed out that some MS legal systems require information requests to be made for any crime where there is any reason to believe that a person, or evidence, is to be found in another MS. This has resulted in enquiries being made in cases which would be regarded in both MS as minor offences.

During the course of the Study it became clear that there were widespread gaps in the quantitative statistics available within MS (both with law enforcement agencies and collectively) regarding the numbers and, equally importantly, categories of information exchanges made between MS. There were also quite a few comments about the varying types of requests and replies which were being exchanged and the resulting differing levels of effort required to comply with a request, or – equally importantly – to make use of the information provided to assist another MS or specific agencies within it.

There are automated HIT/NO-HIT exchanges, or more accurately, data requests, seeking confirmation of whether a person is wanted or missing (see the INTERPOL databases categories described in this Report for further details of the types of data). Additional examples would be “operational” information details which require a request to another MS. That MS can then often, but by no means always, immediately access the information in its own or other immediately accessible databases.

Obvious examples of basic operational information include whether the receiving MS service knows of the subject(s) of the enquiry, and if so what the information is, especially when it is purely factual, e.g. "is Mr. X wanted for any alleged offences", or additionally "Mr. X is driving car ABC123 and says it is his car - is it?" Generally speaking, automatically obtained information or basic operational information can often be delivered quickly and without major resource efforts, though again this is not always the case.

Further enquiries, beyond the basic technical and operational information, typically require considerable allocation of resources. These might involve judicial requests (e.g. responses to Rogatory Letters) which will require more personnel input, or alternatively the gathering of data from several sources within an agency or among national agencies, and the transcribing of this information in an appropriate manner before sending the reply. Some requests involve the allocation of very considerable resources, such as the interviewing of witnesses, often under strict judicial control. Examples would include surveillance operations or the taking of statements, especially in complex financial criminal investigations or prosecutions.

Inclusion of these categories of requests in the "administrative registers" or "logbooks" the project recommends establishing on national levels should be considered. The types of categories would ideally be agreed centrally by all the MS, also in view of the benefit of comparable statistics, but might well include:

- basic automated HIT/NO-HIT enquiry on a central database (such as SIS data on wanted persons)
- enhanced basic HIT/NO-HIT data which can be automatically or semi automatically obtained (e.g. simple yes/no anything known requests, or available "identity corroboration" data such as telecommunication subscriber and vehicle registration data
- disclosure of "known data", i.e. details of convictions and information or categorised intelligence[18]
- EAW enforcement requests and related replies (obviously this will generally be already held and easily accessible, and would be recorded on a one case, one exchange basis for reasons of simplicity and practicality)
- EIO assistance requests and related replies (again on a one case, one exchange basis)
- MLA requests, for obtaining evidence in relation to criminal investigations or for actual criminal proceedings but where the evidence is not required to be actually presented
- judicial proceedings requests, where the information needed falls into the above category, but is actually intended to be used in court proceedings
- proactive intelligence on specific persons or companies, i.e. supplied without a specific request (EUROPOL, INTERPOL, and OLAF would typically be receivers or suppliers of such exchanges)
- proactive intelligence on trends, where the main purpose is not to supply or seek information on specific individuals (care would be needed to avoid double counting with proactive intelligence on persons or companies)

[18] ECRIS and EPRIS data might be subsumed under this category, or separate items to better understand the levels of exchanges of these systems if and when they are implemented

In many cases such information on exchanges already exists, but it is typically not necessarily available in one location, nor are the respective definitions for the more subjective types of information exchange category harmonised.

3.5 Communication channels and information flows

Various communication channels exist for cross-border information exchange in the Member States; bilateral, multilateral and at the level of the EU, each designed for its own purpose.

In the past, law enforcement officers who wanted to communicate with their counterparts across the borders could have chosen between two types of channels, an informal and a formal one. The INTERPOL channel was the most commonly used formal communication channel in the past. However, other very important channels such as SIRENE, EUROPOL, Customs Information System relate exchange, liaison officer networks, etc., have complemented and enriched the exchange of information among law enforcement authorities across the European Union, and sometimes MS indicate there are already too many communication channels.

During the last decade, the number of information exchanges has increased significantly. In correlation to this, the number of communication channels through which information can be exchanged has also expanded. Apart from the above mentioned channels, many bilateral and multilateral initiatives were set up in order to facilitate the exchange of information and to supplement the existing EU communication channels. Furthermore, the technical means by which communication can take place has been enlarged at the same time, and currently includes direct data communication links, e-mails, ordinary mails, telex, telephone channels, etc.

The latest developments sometimes make it more difficult to know which channel, and what means of communication, should be used for the cross-border exchange of information in a specific case, and sometimes the use of different communication channels causes significant but certainly not intolerable levels of communication duplication. However, while mentioning communication channels, the informal networks consisting of the well known “old boys’ network”, built on personal relationships, should not be forgotten. Although “old boys’ networks” are not a part of any legal instrument, they do in reality complement and facilitate existing cross-border exchange of information among the EU MS.

Almost all law enforcement authorities communicate and exchange information through their specialized and centralised departments for international cross-border co-operation and exchange of information (e.g. EUROPOL National Units, the INTERPOL National Central Bureaus, the SIRENE Bureaus, Customs and Excise authorities, etc.) by using different communication means and different communication channels. There is no “universal means”, nor is there a “universal channel”. Despite this, the roles of Police and Customs Co-operation Centres shall not be overlooked. They play a significant role, especially in border regions, and complement national centralised departments and avoid the risk of being dependent on one information exchange organisation or one system, which may have technical limitations or operational gaps.

The variety of communication channels may lead to confusion, but most MS do not have difficulties in choosing communication channels, especially where clear (national) handling instructions, or handbooks and guidelines regulating the international cross-border information exchange are in place.

Many of the Focus Countries expressed concern at the lack of proactive delivery of information which might be of use to the receiving rather than the requesting country. While greater co-operation between and with EUROPOL and OLAF is highly desirable - and the opportunities are becoming steadily greater - past experience suggests proactive delivery of information will not occur without being incorporated into formal performance measurements. The OLAF AFIS systems, especially CIS, were felt by several MS to hold very limited data, but it has to be stressed that the system is dependent on MS themselves to submit information in the first place. Other channels face similar difficulties: at the moment there is approximately 100,000 DNA data and 100,000 fingerprint data available and provided by MS to the INTERPOL DNA and fingerprint databases, although single MS dispose with significant quantities of this kind of data, but do not share them with other MS. Moreover, even some third countries (non EU) supply more information to EUROPOL than some large EU MS.

The law enforcement communication channels can be, and often are, divided along the lines of roles and users. The communication channels are often typically divided between "police communication channels" and "customs communication channels". However, these distinctions should not be regarded as strict because police authorities may have access to customs communication channels and vice versa. However, "police communication channels" are mainly used by police authorities and "customs communication channels" by customs and excise authorities. While areas of direct overlapping interests are often limited, in practice police and customs will have many information sources of mutual interest, especially regarding large scale organised crime involving significant numbers of people and commercial organisations.

3.5.1 Police Channels[19]

3.5.1.1 EUROPOL - EUROPOL National Unit & EUROPOL Liaison Officer

The EUROPOL communication channel is one of the most widely used communication channels among the EU MS, as well as third countries which have signed agreements with EUROPOL. While EUROPOL's mandate is focused on organised crime, this does not in practice seem to result in any problems for international exchange of information through this channel.

As part of police co-operation and exchange of information between Member States, EUROPOL:

- facilitates exchange of information between Member States
- collates and analyses information and intelligence
- notifies the competent authorities of Member States without delay via the national units of information concerning them and of any connections identified between criminal offences;
- aids investigations in Member States
- maintains a computerized system of collected information
- helps Member States train their competent authorities
- facilitates technical assistance between Member States
- serves as the contact point for combating euro counterfeiting

[19] The term *Police Channels* should not be understood to mean that only police authorities use those channels for cross-border information exchange. It should be noted also other law enforcement authorities (e.g. Customs) use those channels, though in fact they are mainly used by police authorities.

EUROPOL takes action when at least two Member States are affected by serious international organized crime. This covers an increasing number of areas, namely:

- preventing and combating terrorism
- drug trafficking
- trafficking in human beings
- illegal immigrant smuggling
- trafficking in nuclear and radioactive substances
- motor vehicle crime
- counterfeiting and forgery of means of payment
- money laundering (except for predicate offences)

Communication with EUROPOL almost always takes place through the EUROPOL National Units that can exchange information with each other directly or forward information to their respective EUROPOL Liaison Officers. The authority responsible for cross-border exchange of information is the EUROPOL National Unit and for that reason the EUROPOL Liaison Officer in The Hague is not considered a Liaison Officer stationed abroad but is treated as a part of the National Unit.

The EUROPOL National Units perform the following tasks:

- Supply EUROPOL on their own initiative with the information and intelligence necessary for it to carry out its tasks
- Respond to EUROPOL's requests for information, intelligence and advice
- Keep information and intelligence up to date
- Evaluate information and intelligence in accordance with national law for the competent authorities and transmit this material to them
- Issue requests for advice, information, intelligence and analysis to EUROPOL
- Supply EUROPOL with information for storage in the computerised system

The EUROPOL Liaison Officers receive information provided by the EUROPOL National Units and forward it to the relevant EUROPOL Liaison Officer(s) of other EU Member States at EUROPOL's headquarters.

In accordance with the EUROPOL guidelines, response shall be given for:

- Urgent requests – within 24 hrs
- Non urgent requests – within 10 days
- Other requests – within 30 days

Information and criminal intelligence, sent from one MS to another through the EUROPOL communication channel, can be sent through and combined with other communication channels as well. In addition, the requests related to the "Swedish Initiative" can be transmitted through the EUROPOL channel, and the time limits set in the "Swedish Initiative" should be observed while being transmitted through the EUROPOL communication channel.

Numerous MS desire to strengthen the role of EUROPOL. The role of EUROPOL and its capabilities is sometimes unclear to the officer. Due to this uncertainty, the proper national structures for communication with EUROPOL, and to derive due benefit from mutual information, are not always as developed as they could be. The planned May 2011 access for EUROPOL and EUROJUST to OLAF's EU wide AFIS databases reinforces the argument for greater co-operation with EUROPOL, as it does for similar co-operation with OLAF, whose new MAB system makes data input much easier for MS and should therefore lead to increases in the quantity and quality of customs relevant data, much of which will fall within serious and organised crime definitions.

3.5.1.2 INTERPOL – National Central Bureaus

The INTERPOL I-24/7 system is a global police communication system which connects law enforcement officers from 188 member countries. The purpose of the I-24/7 system is to exchange cross-border information related to criminals and their criminal activities in order to facilitate criminal investigations in different countries, and to ease the exchange of information between LEAs regarding criminal investigations. Intermediate access to the INTERPOL 24/7 system is provided through the INTERPOL National Central Bureaus placed in member countries around the world.

INTERPOL's Command and Co-ordination Centre (CCC) operates 24 hours a day, 7 days a week in each of INTERPOL's four official languages (English, French, Spanish and Arabic). The CCC serves as the first point of contact for any member country faced with a crisis and/or terrorist situation. The Centre's staff monitors INTERPOL messages exchanged between member countries and ensures that the full resources of the Organization are ready and available whenever and wherever they might be needed.

The National Central Bureaus can search and check the data with direct access to the databases containing information on terrorists, fingerprints, fugitives, DNA profiles, lost or stolen travel documents, stolen vehicles, etc. The process of integrating INTERPOL services with national systems has been facilitated through mobile or fixed network devices, called MIND and FIND. These services give direct access to INTERPOL databases on Nominal data, Stolen and Lost Travel Documents, and Stolen Motor Vehicles.

Usually all types of law enforcement information and criminal intelligence are exchanged through the INTERPOL National Central Bureaus placed at the National Police Headquarters. It is almost impossible to list all types of information exchanged through this communication channel. However, the following types of cross-border information are mostly checked or exchanged through this communication channel:

- checks of persons in police data bases and criminal records
- checks of identity documents
- checks of vehicle's ownership by VIN number and number plate
- checks and establishing of addresses
- establishing and verifying a person's identity
- search of DNA profiles

- information on apprehended persons
- information on smuggling of drugs, explosives, weapons
- information on stolen and confiscated vehicles
- information on controlled deliveries
- information on phone numbers
- information on forgery of money
- arrest warrants from third countries and European Arrest Warrants
- information on missing persons
- information on unidentified persons
- information on fraud
- information on child pornography
- information on illegal migrations and trafficking of human beings, etc.

Additionally, INTERPOL provides all its member countries with instant direct access to a wide range of criminal information through a variety of databases. All databases, except that of child sexual exploitation images, are accessible through the I-24/7 Dashboard, a restricted-access Internet portal. An automated search facility (e-ASF) enables member countries to conduct simultaneous searches in the following databases:

- stolen and lost travel documents (SLTD)
- stolen administrative documents
- stolen motor vehicles
- fingerprints (AFIS)
- stolen works of art

In addition, the following main INTERPOL databases are currently available to member countries:

- Nominal Data – contains more than 175,000 records on known international criminals, missing persons and dead bodies, with their criminal histories, photographs, fingerprints, etc.
- Notices – INTERPOL uses a system of notices to alert police to fugitives, suspected terrorists, dangerous criminals, missing persons or weapons threats. In 2009 more than 4,135 arrests were made on the basis of a notice or diffusion (a similar but less formal type of alert).
- Child sexual exploitation images – the International Child Sexual Exploitation Image database (ICSE) contains around 550,000 images submitted by member countries. It uses image recognition software to connect images from the same series of abuses or from the same location and has helped investigators identify and rescue more than 1,453 victims throughout the world.
- Stolen and Lost Travel Documents – holds information on almost 20 million travel documents reported lost or stolen by 145 countries. This database enables INTERPOL National Central Bureaus and other authorized law enforcement entities (such as immigration and border control officers) to ascertain the validity of a suspect travel document in seconds.

- Stolen Administrative Documents – contains information on almost 300,000 official documents which serve to identify objects, for example, vehicle registration documents and clearance certificates for import/export.
- Stolen Motor Vehicles – provides extensive identification details on approximately 6.2 million vehicles reported stolen around the world. In 2009, more than 26,400 stolen motor vehicles were identified using the database.
- Stolen Works of Art – allows member countries to research records on nearly 35,000 pieces of artwork and cultural heritage reported stolen all over the world.
- DNA Profiles – contains around 94,000 DNA profiles from 55 countries. DNA profiles are numerically coded sets of genetic markers unique to every individual and can be used to help solve crimes and identify missing persons and unidentified bodies.
- Fingerprints – INTERPOL manages an Automated Fingerprint Identification System which contains more than 101,000 sets of fingerprints and more than 3,000 crime scene marks. Member countries submit fingerprints and crime scene marks either electronically or by mail.
- Fusion Task Force – a database of more than 12,700 persons suspected of being linked to terrorist activities. Some 120 member countries currently contribute to terrorism related matters.
- Counterfeit Payment Cards – holds images of counterfeit cards and corresponding data. Seized cards are categorized and form a standard reference library against which suspect cards can be checked. [20]

One of INTERPOL's most important functions is to help police in its member countries to share critical crime-related information using the organization's system of international notices. The information concerns individuals wanted for serious crimes, missing persons, unidentified bodies, possible threats and criminals' modus operandi.

- Red Notice - To seek the provisional arrest of a wanted person with a view to extradition based on an arrest warrant or court decision.
- Blue Notice - To collect additional information about a person's identity, location, or illegal activities in relation to a criminal matter.
- Green Notice - To provide warnings or criminal intelligence about persons who have committed criminal offences and are likely to repeat these crimes in other countries.
- Yellow Notice - To help locate missing persons, especially minors, or to help identify persons who are not able to identify themselves.
- Black Notice - To seek information about unidentified bodies.
- INTERPOL-United Nations Security Council Special Notice - To alert police to groups and individuals who are targets of UN sanctions against Al Qaeda and the Taliban.
- Orange Notice - To warn police, public entities and other international organizations of dangerous materials, criminal acts or events that pose a potential threat to public safety.

The INTERPOL notices contain two main types of information:

[20] http://www.interpol.int/Public/ICPO/FactSheets/GI04.pdf

- Identity particulars - comprehensive identity details, physical description, photograph, fingerprints and other relevant information such as occupation, languages spoken, identity document numbers, etc.
- Judicial information - for example, any offence with which the person is charged; references to the laws under which the charge is made or conviction was obtained; the maximum penalty which has been or can be imposed and, in the case of the Red Notice, references to the arrest warrant or sentence imposed by a court, and details about the country from which the requesting country will seek the fugitive's extradition[21]

The INTERPOL 24/7 system also enables member countries to access each others' national databases using a business-to-business (B2B) connection.

3.5.1.3 SCHENGEN INFORMATION SYSTEM – SIRENE

The SIRENE Offices (Supplementary Information Request at the National Entry) are responsible for the exchange of supplementary information related to the Schengen Information System (SIS) data. The SIRENE Offices are the contact points of each Schengen Member State for SIS and they are operational 24/7.

Exchange of information among the SIRENE Offices is based on the exchange of forms through the SIS NET channel and the supplementary information exchanged through the SISNET e-mail. SIS contains only those categories of data which are supplied by each of the Member States, i.e.

- persons wanted for arrest for extradition purposes (Art. 95)
- third country citizens to whom entry to the territory shall be refused (Art. 96)
- missing persons (and persons needed to be placed under protection) (Art. 97)
- persons summoned to appear before the judicial authorities, including witnesses, or due to be served with a criminal judgement. or to serve a penalty (Art. 98)
- persons due to be subject to discreet surveillance or a specific check (Art. 99)
- vehicles, persons, boats, aircraft and containers being subject to discreet surveillance or a specific check (Art. 99)
- vehicles, firearms, (issued and blank) official documents and banknotes to be seized or used as evidence in criminal proceedings (Art. 100) [22][23]

Police co-operation among the Member States is not limited only to the use of information in the SIS. Moreover, the SIRENE Offices of the Member States exchange any useful information, whilst respecting any national measures taken to implement Articles 39 — 46 using the SIS-NET e-mail, and keep each other informed of measures taken at national level, and of the subsequent amendments to these measures. A HIT may lead to the discovery of an offence or a serious threat to public security. Accurate identification of a subject may be essential, and the exchange of supplementary information, e.g. photographs or fingerprints, is a particularly important factor.

[21] http://www.interpol.int/Public/ICPO/FactSheets/GI02.pdf

[22] The Schengen acquis - 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, *Official Journal L 239 , 22/09/2000 P. 0019 – 0062*

[23] Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism

Further to the SISNET email communication channel, additional channels can be used for exchange of information among SIRENE Offices (i.e. fax, telephone or regular post).

3.5.1.4 LIAISON OFFICERS

Liaison Officers stationed abroad are also examples of communication channels used by different law enforcement authorities engaged in cross-border information exchange. Other communication channels often refer to Liaison Officers stationed abroad in embassies in other EU Member States and in organizations such as FRONTEX, SECI Centre, etc. Liaison Officers often communicate by using host country language and this has an important advantage, as the language barrier is one of the biggest hindrances in cross-border information exchange. Moreover, some liaison officers even have language assistants who enable even faster communication between them and the host country's law enforcement authorities.

There is a growing trend among MS for Liaison Officers to be used for assistance on complex matters rather than simply passing on information delivered through normal channels.

3.5.1.5 FRONTEX

The European Agency for the Management of Operational Co-operation at the External Borders of the Member States of the European Union (FRONTEX) was established by the Council Regulation (EC) 2007/2004 of 26 October 2004 with a view to improve the integrated management of the external borders of the Member States of the European Union.

The activities of FRONTEX are intelligence driven. FRONTEX complements and provides information to the national border management systems of the Member States, whilst fully respecting the principle that the main responsibility of the control and surveillance of the external borders still lies with the Member States.

FRONTEX performs the following main tasks:

- Co-ordinating operational co-operation between Member States in the area of the management of external borders;
- assisting Member States on the training of national border guards, including the establishment of common training standards;
- carrying our risk analysis;
- following up on the development of research relevant for the control and surveillance of external borders;
- assisting Member States in circumstances requiring increased technical and operational assistance at external borders;
- providing Member States with necessary support in organising joint return operations;
- deploying Rapid Border Intervention Teams in order to provide support for Member States for a limited period of time in exceptional and urgent situations;
- management of technical equipment; to set up and maintain centralised records of technical equipment for the control and surveillance of external borders belonging to Member States, which they, on a voluntary basis and upon request from another

Member State, are willing to make available for that Member State for a temporary period.

The main platform of information exchange of FRONTEX is exercised during the implementation of joint operations and the running of its Risk Analysis Network. However, it must be stated that FRONTEX access to intelligence information is narrow since the Agency possesses limited admittance to gather and analyse personal data. Based on the findings of the recent external evaluation[24] of FRONTEX, personal data is communicated via existing channels (mainly via EUROPOL) during joint operations. Even if FRONTEX officers perform interviews, the gained intelligence is accessible only for EUROPOL and MS. However, it should be mentioned that FRONTEX still possesses some rights to access personal data in relation to the implementation of joint return operations as stated in point 9 of the preamble of the Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union[25]. In line with the legislation and the opinion of the European Data Protection Supervisor, FRONTEX may only access and use personal data in order to adequately perform its duty under the above mentioned law, under condition there is a legal basis which specify the necessary and appropriate safeguards, limitations and conditions under which such a processing of personal data would take place, following an assessment of the necessity and proportionality of such measures[26].

Exchange of strategic information is carried out via FRONTEX Risk Analysis Network – members of the network receive relevant data and analysis regularly in co-ordination with the FRONTEX Risk Analysis Unit.

3.5.1.6 FADO - False and Authentic Documents Online

A computerised image-archiving system to help combat illegal immigration and organised crime has been adopted by the Council[27] on the basis of Article K.3 of the Treaty on European Union concerning the setting up of a European Image-Archiving System (FADO).

FADO is a European image-archiving system for the purpose of exchanging - by computerised means and within very short periods of time - information, which the Member States of the European Union possess concerning genuine and false documents that have been recorded. The system's database contains amongst other things (Article 2):

- images of typical false and forged documents;
- images of genuine documents;
- summary information on forgery techniques;
- summary information on security techniques.

[24] External evaluation of the European Agency for the Management of Operational Co-operation at the External Borders of the member States of the European Union, Final report January 2009. COWI A/S

[25] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data applies to the processing of personal data by the Agency.

[26] Opinion of the EDPS on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)

[27] Council Joint Action 98/700/JHA of 3 December 1998

A computerised system with restricted access has been built that enables fast and secure information exchange between the General Secretariat of the Council of the European Union and between the European Union member states and Iceland and Norway.

Part of the information contained in Expert FADO is available to document checkers via the system iFADO - intranet False and Authentic Documents Online. A further reduced portion of the information contained in FADO is being selected by European document experts to be made available to the general public by the General Secretariat of the Council of the European Union on the site PRADO - Public Register of Travel and Identity Documents Online.

3.5.2 Customs channels

Customs Services are typically much smaller than police forces in all MS. This has disadvantages but also an advantage, as the “old boy network” is often closer and more stable than in larger organisations. Much information is exchanged informally in this way and then entered onto national MS criminal investigation and criminal intelligence. Some MS Customs services also have their own LOs or seconded experts in the World Customs Organisation (WCO) HQ in Brussels or the WCO’s EU located regional offices in Cologne and Warsaw, and – increasingly - at EUROPOL, as much Customs crime falls within EUROPOL’s remit.

There is, and must be, close co-operation by Customs Services and other LEAS (typically police or “national crime units” with EUROPOL and INTERPOL) as the nature of Customs offences is such that they will often involve organised crime related information which falls within EUROPOL’s remit. Therefore there is a need for closer co-operation between EUROPOL particularly and OLAF, and it is very encouraging to note that from May 2011 EUROPOL and EUROJUST will have direct secure access to the AFIS systems operated by OLAF, which already exists as Co-operation Agreement at Directors General level with EUROPOL. This is especially so regarding both money laundering itself (especially in view of the recent introduction of EU wide measures for controlling the movement of large sums of cash to, from and within the EU) and the predicate offences underlying the money laundering offence.

The “Customs Channels” for exchanging information are complicated by the fact that the competent authorities in MS may often be different. In quite a few MS judicial proceedings related exchanges are carried out by the police (if not by judicial authorities themselves). This may also extend to criminal intelligence exchanges. Therefore, customs may often exchange with police, and police with customs. This can, as related elsewhere in the Report, cause delays and misunderstandings. Some MS Customs Services stressed that they received better co-operation where the exchanges were with Customs or specialised police units. The increasing co-operation between MS and EUROPOL is therefore to be greatly encouraged. Even more encouraging will be the introduction of EUROPOL and EUROJUST access to the EU wide Customs Information System (much of which is also copied to the WCO, with deletion of personal details) so that it is available to third countries via WCO.

Bilateral and multilateral exchanges of information for criminal investigation purposes are exchanged under standard MLA procedures, with each MS’ national judicial procedures requirements applying. The following comments refer to both Customs Services and those other services carrying out Customs work.

EU specific administrative assistance procedures (MAA) and to some extent MLA procedures are carried out under the Customs Information Systems (CIS) Convention under Council Regulation 515/97, as amended. This authorisation applies for 1st Pillar matters, i.e. the prevention and detection of offences against, and losses to, Community Customs legislation and to the Community Budget.

The 1997 the Naples II Convention, which most MS felt was the basis for their exchanges, covered mutual assistance within both the MAA AND MAA domains regarding 3rd Pillar matters, i.e. judicial proceedings and penalties in relation to 1st Pillar matters, and for the prevention and detection of offences and violations of national Customs Laws in MS. OLAF and MS have pointed out that clarification of the nature of the matters for which information is exchanged is key to the success of the exchanges (1st Pillar or 3rd).

3.5.2.1 CUSTOMS INFORMATION and RELATED AFIS SYSTEMS

The Customs Information System (CIS) Convention authorises the establishment of EU wide intelligence systems and the creation of a register of criminal investigations in Customs matters. The resulting Anti Fraud Information System (AFIS) databases, including the Customs Information System itself, are operated by OLAF which is responsible for setting up a network of (MS) LOs in each MS and for all IT aspects in as much as they can be controlled from the centre. The systems offer secure encrypted transmission capabilities and secure encrypted computer terminals. OLAF also has an extensive team of analysts who use strategic, operational and tactical intelligence skills and related experience, alongside analytical tools software such as i2 Analysts Notebook to carry out proactive and reactive analyses for strategic, operational and tactical purposes, either independently or in co-operation with one or more MS.

All MS administrations inputting to and using AFIS must meet common quality and completeness standards, which are overseen by OLAF. Given the very considerable advances in user friendliness introduced from June 2010 by the Mutual Assistance Broker (MAB), a simultaneous multiple database input system for reporting suspicions, detections, seizures and investigations (including judicial proceedings), and especially the May 2011 implementation of granting EUROPOL and EUROJUST access to AFIS systems, it is clear that OLAF is an equivalent of EUROPOL for Customs matters which fall within the remit of the EC by being related to their own resources, i.e. Customs duties which are collected by MS on behalf of the EC rather than being revenues of MS. Therefore, greater involvement of OLAF, together with EUROPOL, in MS wishes for information exchange modernisation should be considered throughout the follow up actions relating to the findings of this Project.

The systems within AFIS are:

- Customs Information System (CIS) – the main information and intelligence database
- FIDE (Customs Files Identification Databases) the register of criminal investigation cases on Customs matters – this responds to MS inputting identification details, including national case registration number, together with brief details of the circumstances
- MARINFO (suspicious movements and inspection data, suspicious circumstances and seizures in relation to large vessels including major river traffic)

- YACHTINFO (as MARINFO, for smaller vessels, typically involving excise goods and drugs seizures – the latter often being for sizeable amounts)
- CIGINFO (seizures, suspicious movements and circumstantial data relating to cigarettes and other tobacco related products)

The main information categories stored and exchanged for both known or suspected offences related to MS interests or those reported in relation to EC interests:

- Businesses
- Persons (such data is not transmitted to WCO for use in its CEN systems)
- Commodities
- Means of transport (including Vehicle and Chassis registrations)
- Fraud trends
- Retained (detained for investigation, seized and confiscated consignments)

The nature of Customs Criminal Investigation and Criminal Intelligence records is such that they involve the storage of much data. A complication is that this has resulted in more detailed but smaller scope (geographic, themed) databases such as the Marinfo ships and maritime cargo database being created. Information on these databases is regularly updated and viewed multilaterally and bilaterally. There has, however, been a major need to simplify the procedures, by enabling simultaneous multiple input to several systems (e.g. Marinfo, Ciginfo, CIS itself and FIDE) to ensure “one case means one report”, creating several cross referenced records from one input.

At present OLAF is co-ordinating the introduction of such a system – the Mutual Assistance Broker System, introduced from 15th June 2010 and for which OLAF has provided extensive introductory training for MS. Follow up progress will be monitored by OLAF together with the named AFIS LO in each MS.

The success of MAB would be a very major step forward for the co-ordination of Customs information exchanges, and for future further co-ordination with EUROPOL and EUROJUST. MAB will also offer opportunities for much quicker central EU wide recording of much data from domestic master information and intelligence databases and mini databases.

However, this is a demanding remit. OLAF has pointed out that much of the data currently entered onto the AFIS databases via MAB (a secure system) is historical data being reinserted, and is not proactive data (e.g. intelligence about actual or suspected trends, new circumstances) despite the CIS Convention making it clear that MS shall send in unsolicited data.

It is therefore clear that one indication of the success of MAB and of wider improvements in MS multilateral and bilateral co-operation would be in significant increases in the numbers of inputs onto AFIS systems, including FIDE, together with early analysis of the quantitative and qualitative results, either by MS analytical units, groups of analytical units, or OLAF’s units, or combinations of these groups.

It is likely that at least a year's input would be needed to obtain a definitive assessment, and this would imply evaluation from June 2011. Conveniently, this would enable comparisons to be made with the period after 27th May 2011, i.e. when EUROPOL and EUROJUST have AFIS access, and especially for early identification of this access leading to early input by EUROPOL and EUROJUST (i.e. genuine sharing of information).

Customs services often participate in JIT operations, which in wider definitions include joint monitoring and interception exercises for sensitive goods (typically excise goods). Central dissemination of the results of these exercises could be enhanced by ensuring their entry onto AFIS systems via MAB, entry onto FIDE if criminal investigations result, and co-operation with OLAF on analysis of results during and after the exercises through the use of OLAF's Virtual OCU (Virtual Operations Co-ordination Unit) whose staff cannot participate in MS' exercises but can observe and act as technical experts. Such participation seems a highly cost effective way of ensuring wider dissemination.

Several MS expressed concerns about the limited volume and detail of data on AFIS systems. However, such input is dependent on the MS themselves and there was widespread support for the introduction of simultaneous multiple database input through MAB.

In conclusion, regarding the future of Customs co-operation (especially regarding the maximisation of the potential offered by MAB and the granting of direct access to AFIS for EUROPOL and EUROJUST) it is important to stress that the AFIS systems, especially FIDE, have the potential to act as "central registers" without compromising the jurisdiction of MS. OLAF does not have viewing rights to FIDE, which records criminal investigations (as the supplied data is exclusively within the jurisdiction of MS and therefore ownership of the data remains with MS).

It is also clear that the currently limited information held on CIS needs to be significantly increased by ensuring that appropriate staff and units have sufficient incentives to provide information proactively, which may only be of direct benefit to another MS. This challenge applies beyond Customs.

3.5.2.2 FIU NET

Further to the reasons mentioned above explaining why Customs offences and intelligence information are likely to be frequently relevant to EUROPOL regarding organised crime issues, such data will typically involve very close relevance to the work of the MS units comprising the Financial Intelligence Units of the MS (the FIU Net). All evaluations of the quantity and quality of all bilateral and multilateral formal information exchange systems, especially CIS and MAB technical and procedural upgrades, must take account of the effectiveness of co-operation with FIUs. This includes informal as well as formal information exchange procedures.

The United Kingdom (particularly, but not only SOCA) and the Netherlands (including FIOD, under control of the Finance Ministry), which is the "host" country of the wider Egmont Group comprised of EU and many non EU States, have very significant involvements in exchanges of financial information, both internally and across-borders. Therefore these MS should be particularly involved in any reviews of EU wide exchanges of financial information. The actual utilisation of such exchanges involves complicated and resource intensive procedures, and ensuring fully effective measures against such crimes and the involved criminals is a worldwide challenge.

3.5.3 Bilateral and Regional Channels

The exchange of information among the EU MS law enforcement authorities is based on both bilateral and multilateral co-operation agreements. The bilateral co-operation agreements between EU Member States define co-operation in several areas that fall within the competence of law enforcement authorities. Different types of legal documents define bilateral co-operation between EU MS' law enforcement authorities (i.e. treaties, agreements, cooperation agreements, memoranda of understanding, protocols, common declarations, etc).

Bilateral co-operation agreements may be concluded at national and/or regional level of different EU MS and in some cases non EU countries take part as well. Some of them are very detailed, whereas others provide a general framework for cross-border co-operation and exchange of information. However, most of the bilateral agreements contain specific articles concerning cross-border exchange of information between law enforcement authorities in order to supplement the existing EU instruments.

Generally speaking, bilateral or multilateral co-operation and exchange of information takes place at national, regional and local level. P(C)CCs, further described below, or direct communication channels among MS LEA are usually responsible for the co-ordination of the operational actions and for the cross-border exchange of information in specific border areas.

Multi-lateral initiatives, such as the ones described below for illustration, are very cost effective ways of creating a liaison officer network. The focus on their region encourages closer liaison than may sometimes be possible at a wider multinational level due to closer involvement in a more focused range of information exchange activities, e.g. by closer monitoring of multinational special exercises such as movements of stolen cars and cigarettes and weapons trafficking.

- Southeast European Cooperative Initiative (SECI)
  The Southeast European Cooperative Initiative (SECI) was launched as an idea among the Euro-Atlantic co-operation in May 1995 in Vienna. The Southeast European Cooperative Initiative Regional Center for Combating Trans-border Crime[28], the SECI Center, is an operational organization bringing together police and customs authorities which facilitates the rapid exchange of information between law enforcement agencies from different countries regarding trans-border criminal cases.

  The SECI Center's main objectives are:
  - Setting-up a mechanism based on enhanced law enforcement co-operation at national level to be used by the parties in order to assist each other in preventing, detecting, investigating, prosecuting and repressing trans-border crime
  - Supporting the field activities of the law enforcement officers

[28] http://www.secicenter.org/

- Providing assistance to the Parties in order to harmonize their law enforcement legislation in respect to the EU requirements
- Supporting national efforts in order to improve domestic cooperation between law enforcement agencies

The SECI Regional Center Headquarters is located in Bucharest, Romania. The SECI Center co-ordinates regional operations, putting together the resources of the 13 Southeast European member countries in order to dismantle organized crime networks. Member states, i.e. those participating in the exchange of information within SECI are Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Greece, Hungary, F.Y.R. of Macedonia, Moldova, Montenegro, Romania, Serbia, Slovenia and Turkey. Besides the member countries, there are 23 observers, countries and organizations: Austria, Azerbaijan, Belgium, Canada, Czech Republic, EUBAM, France, Georgia, Germany, Israel, Italy, Japan, The Netherlands, Portugal, Spain, Slovakia, Ukraine, UNODC, UNDP Romania, the United Kingdom, UNMIK, and the United States of America. Italy and the United States maintain permanent representation at the SECI Center, and INTERPOL and the World Customs Organization are permanent (non-resident) advisors to the SECI Center. Further to this, the Observer Status was granted to CARICC - Central Asian Regional Information and Coordination Centre for combating the illicit trafficking of narcotic drugs, psychotropic substances and their precursors in 2010.

The SECI Center operational activities are conducted within the framework of seven Task Forces addressing issues of drugs and human beings trafficking, stolen vehicles, smuggling and customs fraud, financial and computer crime, terrorism and container security. Next to this, the SECI Center issues analysis and reports on specific areas targeting organized crime, and organizes trainings for member countries' law enforcement representatives.

The SECI Center's network is composed of the Liaison Officers of Police and Customs Authorities from the member countries, based in the Center, supported by 13 National Focal Points (NFP) established in each member state. The NFP representatives stay in permanent contact with the liaison officers in the headquarters and keep close relationships with the police and customs authority in the host country. The NFP assure rapid information flow by collecting and distributing the information requests and answers from and to the law enforcement agencies and the headquarters liaison officers. Liaison officers, detached to the SECI, usually communicate through an encrypted communication channel with their NFP.

In 2009, the Convention of the Southeast European Law Enforcement Center (SELEC) was signed by the representatives of the 13 Member States. The SECI Center will transform into SELEC - Southeast European Law Enforcement Center - once two thirds of the Member States have deposited their instruments of ratification, acceptance and approval. The SELEC Convention will enable the Center to create an enhanced analysis capacity with a broader data system and an adequate level of protection of personal data in accordance with EU requirements.

SELEC will:

- Support investigations and crime prevention activity in Member States
- Facilitate the exchange of information and criminal intelligence and requests for operational assistance
- Notify and inform the National Focal Points of Member States of connections between suspects, criminals or crimes related to the SELEC mandate
- Collect, collate, analyze, process and disseminate information and criminal intelligence
- Provide strategic analysis and to produce threat assessments related to the SELEC objective
- Establish, operate and maintain a computerized information system
- Act as a depositary of good practice in law enforcement methods and techniques and to promote the same through multi-national training and conferences for the benefit of Member States

- Nordic Co-operation – is based on mutual trust and recognition of criminal law enforcement systems. Within this model, there is an intense police and customs co-operation that has only a limited basis in formal agreements or statutory law. The information that the police and other agencies are allowed to exchange with their national colleagues may be exchanged with their Scandinavian colleagues as well. They may use direct contact as well as a detailed network of liaison officers (PTN network), which not only represent and answer requests for their own country but for all countries of the Nordic Co-operation. All the Nordic States and their neighbour states stressed the importance of this seamless co-operation.

- Task Force on Organised Crime in the Baltic Sea Region[29]
  The Task Force created in 1996 is not a permanent body but a network for operational cooperation and its support. Countries participating in this network are Denmark, Estonia, Finland, Germany, Iceland, Latvia, Lithuania, Norway, Poland, Russia and Sweden, whereas operational cooperation is also sought with relevant law enforcement authorities from the countries falling within the operational scope of the Baltic Sea region, but not being members of the Task Force. In addition, close cooperation with EUROPOL, EUROJUST, INTERPOL, FRONTEX and the European Commission is sought. Objectives include minimisation of duplication of efforts and routing the information flow into one common channel when it comes to intelligence. The meetings of the Task Force, which consists of high level representatives of the government, take place once or twice annually. The Task Force has the role of approving the proposals for joint measures received from its Operative Committee (OPC).

  The OPC is a multidisciplinary body consisting of permanent representatives from police, border/coast guard authorities, customs and national prosecution offices from each Baltic Sea region country. Any other relevant authority may be added by countries if necessary. The OPC works in close cooperation with senior analysts as permanent network with members nominated by each country in the region, facilitating exchange of experiences and best practices, proposing either political or legislative solutions, finding

[29] http://www.balticseataskforce.ee/

and distributing financing for the operations and coordinating joint operations. The senior analysts are in regular contact and exchange risk assessment and crime related information.

The Task Force cooperation uses the cycle of EUROPOL's Organised Crime Threat Assessment (OCTA). While the OCTA itself is used for appropriate strategic planning taking into account the findings relevant to the region, the individual national contributions are exchanged between Task Force countries and additionally analysed in depth by the senior analysts taking part in OCTA delivery process. The goal is to support nationally or regionally important but on European level minor issues. For this purpose the network also liaises with other similar initiatives such as the Nordic OCTA prepared within the Nordic police and customs cooperation group.

The chairing country, which changes every two years, regularly informs the EU Police Chiefs Task Force, EU Council's Multidisciplinary Group on organised crime, EUROPOL's Management Board and the Council of Baltic Sea States (CBSS) about the findings and results of Task Force and Operative Committee activities. The chairing country provides the Task Force with a permanent Secretariat.

- The Exchange System for Legal Information (ESLI) is being used for the exchange of information between The Netherlands, Belgium and Germany. It enables the users to register a question (about people, incidents, vehicles etc) and send it to known participants in another office (domestic or abroad) via a secure line.

  ESLI is the application used by the police co-operation centre at the Dutch border town of Heerlen, The Netherlands, to handle information requests. The ESLI application is used to log requested information, to transfer requests to the appropriate police officer, to allow the receiving officer to introduce the response, and to transfer back to the requesting MS.

- Linguanet was first developed for police and emergency services working at the Channel co-operation between the UK, France, The Netherlands and Belgium. Later it was expanded and nowadays enables officers to create and transmit routine enquiries and replies to those enquiries quickly. It uses pre-formatted messages, designed by police, for topics such as persons, vehicles and firearms and free text information may also be sent.[30]

- COASTNET is used by the Baltic Sea Region Border Co-operation and is an electronically encrypted system operating 24/7 via the internet. The main purpose of COASTNET is to exchange information related to maritime border illegal activities such as illegal migration, smuggling of goods, false documents, stolen navy equipment, protection of fishing areas, environmental protection, navigation, security. The type of information exchanged through COASTNET concerns mainly text files, pictures as well as documents in PDF format.

[30] http://www.prolingua.co.uk/Linguanet/index.html

COASTNET is used in the framework of the Baltic Sea Region Border Co-operation between the border services of Poland, Russia, Lithuania, Latvia, Estonia and Finland, the coastguards of Sweden and Norway, and the police of Germany, Denmark and Norway. English is the language used for information exchange through COASTNET. In each country where COASTNET is used a National Contact Point was created, where the system is available on a stationary computer, principally in operational 24/7 centres. COASTNET caters for multilateral information exchanges, but also provides the possibility to exchange information at a bilateral level only.

3.5.4 Police and Customs Co-operation Centres

P(C)CCs are usually placed in the vicinity of the borders between participating States, either at the border between two EU MS or at the border of EU MS and a third country. Article 39 of the Schengen Convention is the main legal base for the creation of P(C)CCs in the EU. The bilateral and multilateral agreements in many instances further define provisions related to P(C)CCs tasks and cross-border information exchange. The primary mission of the P(C)CCs is to support the operational services and facilitate cross-border exchange of information among the MS concerned. P(C)CCs are therefore a valuable local and regional tool for the expeditious exchange of information and for playing a significant intelligence role catering for operational needs. In addition, P(C)CC's strongly support daily cross-border co-operation and provide quick replies to other LEAs authorities. More and more centres are being established across the Europe.

One of the reasons for creating P(C)CCs is that most centralized international law enforcement structures, like ENUs and NCBs, give priority to serious and organized crime. However, trans-national criminality not only concerns organized crime but also less serious offences such as theft, burglary, etc. frequently perpetrated by criminals residing in the cross-border areas. At the same time, the establishment of P(C)CCs allows for burden sharing between national and regional level and facilitates direct cooperation with neighbouring countries, with which a large number of information is exchanged.

It is clear that P(C)CCs significantly support the exchange of information and criminal intelligence, and provide support to the operational units in border areas. Staff from different agencies of participating and observing Member States overcome formal and usually impersonal administrative procedures between two or more participating states. Moreover, P(C)CCs significantly contribute to a better understanding of the working procedures in participating MS' structures, and staff can consult various administrations' data files and data bases through colleagues who are officers of the MS owning the data. Information and criminal intelligence exchanged via P(C)CCs varies from misdemeanours such as traffic safety and public order matters to illegal migration and other serious crimes. The data which is typically most often exchanged is that on drivers, vehicles, vehicle status, vehicle's ownership, driving licenses, telephone subscribers, validity of identity documents, residence permits and visas, etc. One of the most important advantages is an instant cross-border information exchange which enables a smooth exchange of information and a quick decision making process in LEA's proceedings.

Distribution of responsibilities between national central authorities responsible for international co-operation and P(C)CCs is reasonably clear. While there can be differences between MS, generally speaking there is no overlap when responsibilities are clearly defined and when P(C)CCs' responsibilities do not encroach on those of national units.

Exchange of information and intelligence in P(C)CCs is often seen by MS as direct access to other MS' databases, although in almost all cases foreign LEA officers conduct searches in their national databases and immediately provide results to their counterparts (i.e. indirect access). For example, at one French-Italian P(C)CC the staff has access to 65 different databases and approximately 80 % of cross-border requests are responded to within 4 hours.

Most of the P(C)CCs play a role in the co-ordination and cross-border exchange of information, linked to dealing with criminal activities. P(C)CCs may receive requests from a variety of partners and the police and customs officers usually work together in those centres. Moreover, in some P(C)CCs prosecutors also take part.

A greater connectivity of P(C)CCs across the EU would enhance and facilitate the existing exchange of information at local and regional level. Many P(C)CCs have been striving for the establishment of contacts with other P(C)CCs across the EU in order to exchange experience and working methods and lastly to assist each other where appropriate. This should not be understood as encroaching on national units' responsibilities but as complementary measures for the purpose of improved cross-border information exchange. A more orchestrated approach would be expected to improve the existing information exchange in future.

3.5.5 Use and selection of communication channels

The selection of communication channels varies from country to country and the choice of selection usually depends on the nature and complexity of the individual case. Besides, it should be noted that different communication channels have been introduced for different purposes, and this has an impact on the selection of the communication channel. The selection of communication channels sometimes also depends on the limitations of some channels (EUROPOL activities aim at fighting organized crimes and other serious cross- border crimes).

The selection of the communication channel is mostly done by central authorities and only in a few MS may local units choose or suggest the communication channel to be used. When a request is received via one of the communication channels from abroad, the response is almost always sent back using the same channel and two or more channels are very rarely used for the same requests.

Some Member States mostly use EUROPOL for cross-border information exchanges within the EU (e.g. Bulgaria, France, Denmark) while others prefer INTERPOL (e.g. The Netherlands[31], Estonia, Germany), although SIRENE exchanges may have the most transactions (e.g. Germany, Slovenia). Usually there is a question of whether to use EUROPOL or INTERPOL or even both communication channels, and the selection almost always depends on the peculiarities of each single case. When a third country is involved, the INTERPOL channel is mainly used. Although the EUROPOL mandate somewhat restricts the exchange of information between EU MS and EUROPOL to organized crime matters, the implementation of SIENA has introduced the capability for direct bilateral cross border exchanges on a full range of actual or suspected

[31] Trends are moving toward EUROPOL

crimes. In practice, the current mandate was not mentioned as problem by either the MS or EUROPOL.

Although EU MS use both EUROPOL and INTERPOL for the cross-border exchanges within the EU, the majority of visited MS expressed a wish and tendency to increasingly use EUROPOL for exchanges within the EU and, according to the MS, EUROPOL should be the main communication channel within the EU. This is also in accordance with EUROPOL's main goals, based on the EUROPOL Strategy[32], where it is envisaged that EUROPOL becomes the first platform of choice for Member States to share operational and strategic information through a strengthened ENU/ELO network within secure and user-friendly information exchange communication facilities.

The role of the SIS is neither to replace nor to replicate the role of INTERPOL. Although tasks may overlap, the governing principles of action and co-operation between the Member States under Schengen differ substantially from those under INTERPOL. Therefore, rules[33] have been established for co-operation between the SIRENE bureaux and the NCBs (National Central Bureaux) at national level.

- Priority of SIS alerts over INTERPOL alerts: SIS alerts and the exchange of all information on these alerts shall always have priority over alerts and information exchanged via INTERPOL. This is of particular importance if the alerts conflict.
- Choice of communication channel: the principle of Schengen alerts taking precedence over INTERPOL alerts shall be respected and it shall be ensured that the NCBs of Member States comply with this as well. Once the Schengen alert is created, all communication related to the alert and the purpose for its creation shall be provided by the SIRENE bureaux. If a Member State wants to change channels of communication, the other parties have to be consulted in advance. Such a change of channel is possible only in special cases.
- Use and distribution of INTERPOL in Schengen States: given the priority of SIS over INTERPOL alerts, INTERPOL alerts shall be restricted to exceptional cases (i.e. where there is no provision, either in the Convention or in technical terms, to enter the alert in the SIS, or where not all the necessary information is available to form a SIS alert). Parallel alerts in the SIS and via INTERPOL within the Schengen area are inadmissible. Alerts which are distributed via INTERPOL channels and which also cover the Schengen area or parts thereof (INTERPOL diffusion zone 2) should bear the following indication: 'Zone 2 except for the Schengen States'. In reality, this is not always the case, which leads to redundancies.

The SIRENE bureau of the issuing Member State shall decide whether to pass information on to third States (authorisation, diffusion means and channel). In so doing the SIRENE bureau shall observe the personal data protection provisions laid down in the Schengen Convention and Directive 95/46/EC. Use of the INTERPOL channel will depend on national provisions or procedures.

[32] EUROPOL Strategy 2010-2014, http://register.consilium.europa.eu/pdf/en/10/st06/st06517.en10.pdf

[33] COMMISSION DECISION of 4 March 2008 adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II); Official Journal L123, 08/05/2008, p39-75

The Schengen States shall ensure at national level that the SIRENE bureaux and the NCBs inform each other of hits. The deletion of an alert shall be undertaken only by the authority which issued the alert.[34]

When deciding what communication channels are to be used for cross-border information exchange, LEAs - especially but not exclusively those of large MS - frequently make use of P(C)CCs due to their quick responsiveness, because replies can be obtained immediately or in a couple of hours. In contrast to INTERPOL, EUROPOL and SIS communication channels which are organised and located centrally, P(C)CCs are by definition located regionally, i.e. at or very near the borders. However, the P(C)CCs' role should not be diminished because of this. They provide direct communication of information between MS and central notification, especially within large MS, and it is often via the "incoming" agency at a P(C)CC, i.e. MS to MS, that communication is not from "central" SPOC to "central" SPOC but by collocated staff at P(C)CCs, who then inform their respective central SPOCs. Therefore, P(C)CCs have very important roles, in both bilateral and multilateral contexts. One of the advantages of those P(C)CCs is that each participating country has its own information services available in the P(C)CC. As a result, all the relevant databases, such as criminal databases, traffic databases for identification of car number plates, of the relevant law enforcement authorities of the different countries are present in P(C)CCs. This makes the exchange of information between the law enforcement authorities at the level of the P(C)CCs very flexible.

The quantities of information exchanged through different communication channels are not directly comparable as one channel may be used for alerts, whereas another would be used for the exchange of criminal intelligence (i.e. often fewer exchanges, but those that require more work). At the same time, not all incoming messages are necessarily requests. In addition, many exchanges are also made today by other units such as Joint Investigation Teams, and by other types of exchanges. Moreover, some information and criminal intelligence exchanges are often directly exchanged between specific specialized authorities (antiterrorist units, drugs units, etc) without informing the national authorities for cross-border information exchange.

In order to better capture data on information exchanges, the project team highlights a need for common "Administrative Registers" or "Logbooks" at national level to be set up, whereby all agencies can consult a 24/7 SPOC to see whether information has been exchanged across borders concerning a certain person, company or object and the responsible agency/officer. Identifying that cross border exchange has already been performed will help all relevant agencies that can be quickly contacted.

Some MS stressed that there is no clear EU policy about the selection of communication channels in the EU and MS choose channels according to their best knowledge and experience. However, the fact is that the Manual of Good Practices concerning the International Police Co-operation Units at National Level,[35], drafted by the European Police Chiefs Task Force, defines the criteria for choosing between various international channels (SIRENE, ENU, EIS, NCB) or bilateral or internal law enforcement offices, such as liaison officers network, according to the type of information exchanged or requested. This manual aims to provide guidelines and

[34] COMMISSION DECISION of 22 September 2006 on amending the SIRENE Manual (2006/758/EC)

[35] Manual of Good Practices concerning the International Police Co-operation Units at National Level (7968/08)

examples for the aforementioned units in order to maximize their resources, avoid overlaps and make co-operation with other MS more efficient and expeditious, and the same principles have been introduced in the Guidelines on the implementation of the Swedish Initiative. Nevertheless, it seems that some MS are not fully aware of the existence of this manual or they just use their own national rules, guidelines, handbooks or experiences for selecting of the communication channels. It is to be debated if stronger focus should be given to following the existing guidelines, a new list of criteria on selection of the most appropriate channel be created in the future, or whether the selection of the communication channels should be entirely left to the individual MS.

Coherence of IT channels and databases was raised as an important subject by operational staff that is not in favour of establishing additional channels. Existing channels and existing IT communication networks should be used to their full extent before introducing new ones. Before new databases are set up, an investigation should be started to see if such a solution already exists, either in MS or on a central EU level. The daily life of LEA officials would otherwise become more and more difficult as more databases are introduced. IT should support work rather than complicate it.

Taking this advice on board, one has to look at similarities in terms of IT communication channels and the sort of data used for recording and enquiries. Indeed there are duplications in both fields. EUROPOL operates a dedicated IT network, as does INTERPOL, SISNET is operated by SIS responsible, OLAF’s MAB applications (CIS etc.) are accessible via a network managed by DG TREN, the Prüm automated exchange takes place using s-Testa, a European backbone network also operated by the European Commission is in use for EURODAC for many years and supposed to serve SIS II and VIS. EUROJUST uses a more dedicated secure network and FRONTEX is working on EUROSUR and the secure exchange with their MS contact points. SECUNET for immigration matters and individual IT networks to MS embassies and consulates abroad are only two more of a definitely larger number. In theory, one or the other could be used when one of the IT networks fail, but this is neither currently designed nor practical because access points are often not at the same location, and bandwidths are different, as are encryption methods.

However, it is valid to consider whether harmonisation could be introduced, leading to easier maintenance and lowered costs. Regardless of whether approximately 35 parties outsource labour or use own staff, it is a matter of fact that specialised knowledge of multiple implementations has to be available and personnel have to be on support duty in cases of technical problems. It is certainly not within the objectives of this study to analyse the cost effectiveness and reliability of options. However, it is one of the findings which the Project feels needs to be brought to attention.

There is no doubt that good reasons do exist why various databases hold the same or similar information. In addition to grounds based on legal frameworks, databases have been developed over many years, extended, renewed or replaced by state-of-the-art solutions. This applies to MS who started with IT more than 40 years ago as much just as it does to new developments which have been recently set up or are being set up. From a practical perspective, we face more and more databases, which have to be accessed either to insert new records or to be consulted in order to retrieve information. A wide range of integrators and database developers are in competition and there is no doubt that the free market principles have to be respected. As a result, MS and central services are using different products, each of them certainly chosen carefully. In reality, the problems emerging are not because of different brands and versions but because of the lack of interoperability between systems, completely diverse user interfaces, and different structures holding the same or similar information in different ways. Another aspect, as important as interoperability, is the age, completeness and accuracy of data stored, with direct implications on the usefulness for LEA officials when they retrieve the information. If data are outdated, they may still be required for tracing the chronology or for the purpose of documentation, but they are certainly not helpful when it comes to the quick identification of persons or searching for subjects who have changed their personal details and appearance. The point is that in a number of cases where one agency has recognised the change, the agency would certainly correct their own data, but it is not in the position to amend other authorities' or even other Member States' records.

Since in many MS IT systems are only partly linked by a sort of personal identification number, in some databases the record is updated, while in others the record would not be updated and so would become outdated. Consequently, an inquiry with the actual data will only succeed to a limited extent.

Another phenomenon occurs if a person's details are stored in EU-wide databases. MS A may send a personal record to SIS, INTERPOL, EUROPOL and CIS. No matter how cumbersome the data input was to satisfy all systems, one record has grown to four records which are no longer linked. MS A will probably know the full history until the person commits the next crime in MS B. When MS B retrieves the information from all of the above mentioned systems, the officer has to conclude that the four records belong to the same person. Four records may not be a problem but we have to take into account that several systems may provide more than one record because of extended search algorithms. Frequent names and incomplete sets of data make it even more difficult to exclude the non appropriate ones and to collate those which belong to the person in question. It is not obvious why central systems would not do the same as many national systems and link records where the identity has already been established. If not doing so, the manual process and conclusion will have to be carried out each time the person is subject to an enquiry. The result would be that not only would data be duplicated; so would the workload.

This does not mean that all databases had to be merged or that LEA officials would have unlimited access to all records. Procedures where there is permission to access only those sources which are necessary to fulfil the duties are already implemented and this situation would not change.

Again, it is far beyond this study to investigate pros and cons. However, one could observe the tendency that for "each and everything" a new database has been set up and new ones are in the pipeline. In practical terms, the reliability of the information will diminish from the user point of view if there are no measures to compensate for the flood of information. A 'Google-like approach', presenting incalculable records, is counterproductive in LEA work.

In short, there is a high risk that the trust in the value of new IT systems will decrease resulting in less usage. Given the economic situation in the near and mid-term future, the number of LEA staff is generally not increasing. This is probably the main motivation behind the request for carrying out EU wide investigations of what databases and communication systems are already in place, and therefore to consider whether these can be adapted, before considering setting up new databases and related communication systems.

The baseline is that that existing legal instruments and IT facilities should be better used before introducing new ones.

3.5.6 Relationship between formal and informal methods of exchanging information

Informal exchanges exist in almost all MS although this is not regulated in the legislation. The proportions of informal requests to formal requests for exchange of information cannot be estimated accurately as definitions (and therefore calculations) may vary from country to country. Informal exchanges are almost always followed up with formal requests and it is therefore often possible that informal methods become part of formal procedures. Some countries are more open to informal cross-border exchanges while others try to keep formal control over all exchanges made with other countries. However, the fact is that even central authorities are not always being informed about the exchanges which do take place in their countries at lower levels while some LEAs are authorized to directly exchange information with other counterpart authorities.

Informal exchange usually speeds up responses on existing or delayed information exchanges. Usually, informal exchanges are mainly related to urgent information exchanges, typically through personal phone contacts, and on many occasions informal contacts are made “in advance” in order to find out what kinds of information are available in MS. However, from the legal points of view, informally obtained information of criminal intelligence cannot be used in legal procedures and therefore informal exchanges need always to be complemented by formal exchanges if they are to be of value in judicial proceedings.

Although information received thanks to informal relationships may not be used during the judicial procedure, practical experience unambiguously shows the positive influence of such contacts on the flow of formal procedures. Wider informal communications could be encouraged by a limited and permanent staff of different MS SPOCs as long-lasting personal contacts ensure mutual trust.

3.5.7 Work flows and interconnections of law enforcement systems

One objective of the Study was to investigate whether different work flows exist for the same subject matter and where there are obvious gaps in terms of missing or duplicated procedures. Considering that a workflow consists of a series of processes within a procedure, one would have to distinguish between different levels of case work before making a detailed analysis.

Some basic conditions for comparison have to be determined: the sort of work flows to be looked at, and the level of detail. This triggers a number of additional and rather important questions, such as:

- Are we considering national work flows or cross-border work flows?
- Do we see a workflow as a repeatable procedure for different subject matters or do we want to know if the same subject matter is handled differently?
- Is it fair to map MS with different legal systems?
- Do we want to compare the same or equivalent authorities in different MS, irrespective of their potentially differing national systems or do we want to compare authorities in MS who are dealing with the same kind of cases?
- Is it helpful to compare small and big MS?
- Do MS without third country borders (apart from airports) have the same or other cross-border exchange requirements as those MS who face constant seaport or land border traffic of travellers and goods?
- Is it productive to compare old MS with those who joined the EU in the last round of its extension?

Similar questions apply concerning the interconnection of law enforcement systems.

There may be good reasons why a MS has fewer IT systems and databases than others, or why a MS has a decentralised and fragmented structure compared to a MS with centralised services. Regardless of centralisation or decentralisation, concepts may vary on how to keep the information stored in different systems and databases interconnected or not, and to what degree. The reasons why things are organised in this or that way will mainly be legal conditions, geographical differences, history and age of IT structures, and, not least, the financial capacity of the MS.

Given the complexity of the topics and the timeframe within which the Study has been carried out, the Project realised that it had to concentrate on main subjects. It was considered more useful to focus on information flows rather than on the analysis of single workflow steps. A common overview would better demonstrate the relationships between IT systems and the IT and communication channels used. The results mainly derive from institutional documents, responses from questionnaires and on site interviews, and finally experts' experience and knowledge.

The Project also had to take into account that, particularly in big countries, there is hardly anyone available with knowledge of all national law enforcements' organisational and technical solutions. On the contrary, we observed that in many cases there is only fragmented knowledge about available IT databases and IT networks in MS; a similar situation applies to knowing which are already in place or even in constant use. Even on a European central information exchange level, where one would assume that the number of IT networks and IT systems for similar subjects is finite, the involvement of different agencies and organisations in related subjects makes it difficult to obtain comparable information.

In conclusion, we primarily looked for commonalities in cross-border information exchange between MS and from MS to European Central Services. The most suitable framework for the comparison on national level is the information obtained from the three case studies included in the questionnaire:

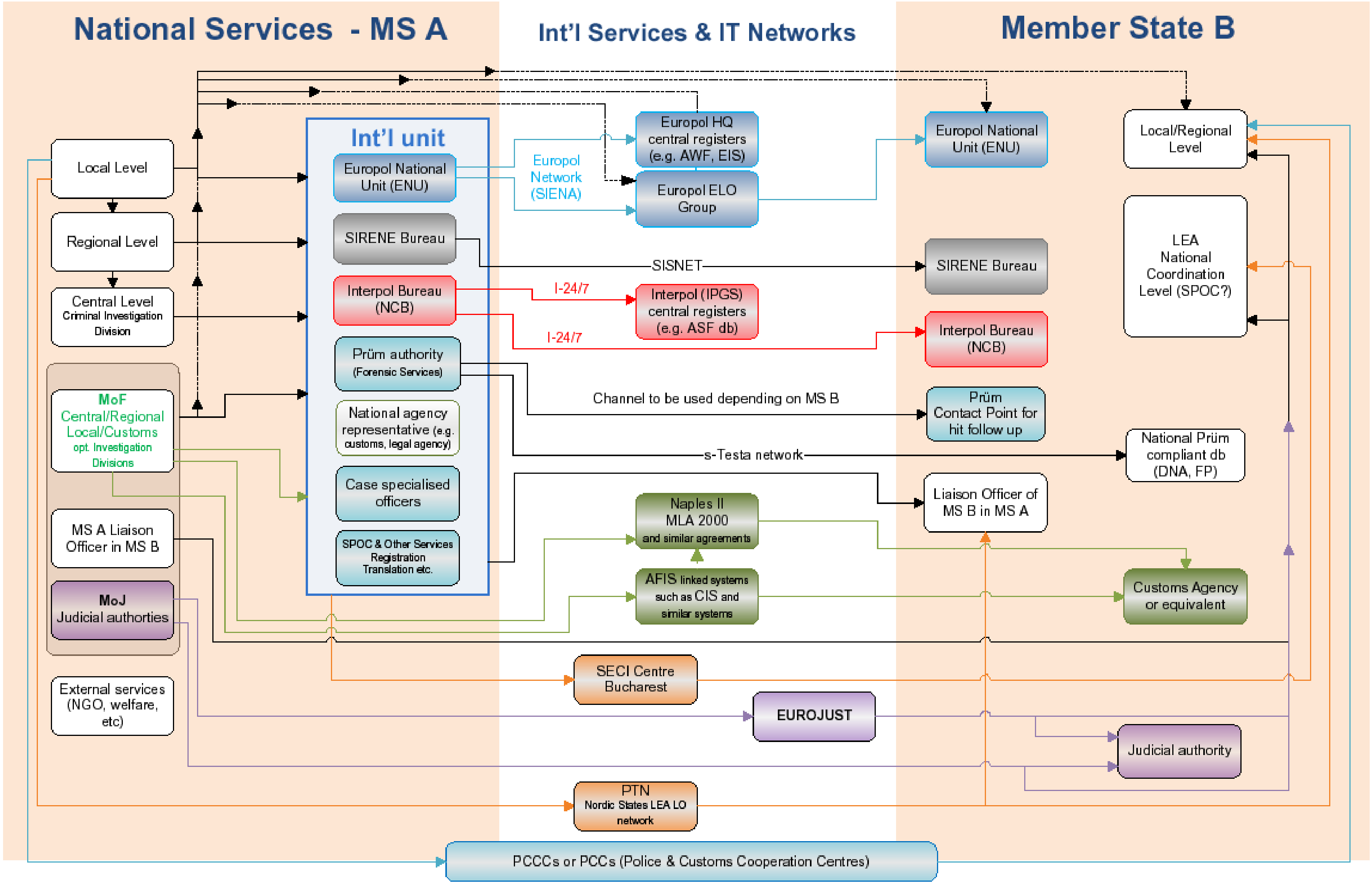
CS 1.:	Trafficking in Human Beings, including child trafficking
CS 2.:	Drug smuggling & trafficking of stolen vehicles
CS 3.:	Computer-related crime (phishing)

The first steps of action depend on how, where and from whom the information was received. In some MS LEAs are expected to act autonomously, whilst in other MS the information has to be forwarded to the appropriate decision making authority. Although in most MS IT structures do exist, the use of phone and fax is still common for urgent actions. This is especially the case in those countries where forces are under different umbrellas which may well differ from those in other, and especially neighbouring, MS. For example, if a customs authority in a port area is not electronically connected to the border police, they are most probably also not linked to the criminal police IT services or to the authority dealing with organised crime. Forwarding information and identifying the right LEA party may imply the risk of certain delays and breaches of confidentiality.

Although not explicitly stated in all responses to the questionnaire, it is apparent that acquired information would firstly, as far as officials are permitted, be used for searches in national IT systems and in international systems. Some MS benefit from central administrative registers where records with basic case information refer to prior or present files. This helps avoid duplication whilst providing identification of the leading agency. The search results in any of the databases may already influence the choice of the channel for cross-border exchange. Depending on the language skills available, written requests to other MS may have to pass through a translation service which can belong to the LEA or can be an external trusted company. Apart from the most important police channels INTERPOL, EUROPOL and SIRENE, Nordic States would probably make use of their PTN network while some New Member States in south-eastern Europe would employ their SECI contacts.

The chart on the next page shows the most important internal connections which may exist in MS, their links to international services and some direct channels to other MS.

LEA MS to MS information exchange, global view



National Services - MS A

Int'l Services & IT Networks

Member State B

Local Level

Regional Level

Central Level
Criminal Investigation Division

MoF
Central/Regional Local/Customs
opt. Investigation Divisions

MS A Liaison Officer in MS B

MoJ
Judicial authorities

External services (NGO, welfare, etc)

Int'l unit

Europol National Unit (ENU)

SIRENE Bureau

Interpol Bureau (NCB)

Prüm authority (Forensic Services)

National agency representative (e.g. customs, legal agency)

Case specialised officers

SPOC & Other Services
Registration
Translation etc.

Europol Network (SIENA)

Europol HQ central registers (e.g. AWF, EIS)

Europol ELO Group

SISNET

I-24/7

Interpol (IPGS) central registers (e.g. ASF db)

I-24/7

Channel to be used depending on MS B

s-Testa network

Naples II
MLA 2000
and similar agreements

AFIS linked systems such as CIS and similar systems

SECI Centre Bucharest

EUROJUST

PTN
Nordic States LEA LO network

PCCCs or PCCs (Police & Customs Cooperation Centres)

Europol National Unit (ENU)

Local/Regional Level

LEA National Coordination Level (SPOC?)

SIRENE Bureau

Interpol Bureau (NCB)

Prüm Contact Point for hit follow up

National Prüm compliant db (DNA, FP)

Liaison Officer of MS B in MS A

Customs Agency or equivalent

Judicial authority

Case study 1:
In case study 1 we assume that an agency in MS A receives information that a person residing in MS B is involved in trafficking of children for forced begging in MS A, transported through a neighbouring MS C. The suspect may be member of an organised crime group.

Most MS report that, after basic checks have been performed, INTERPOL and EUROPOL would be contacted. SIRENE may be involved if a SIS consultation results in a HIT.
Depending on the available technical means there are different methods of gathering information from international services.

- Phone, fax and normal email
- Secure email to the ELOs at EUROPOL The Hague; with a few exceptions, the National EUROPOL Unit (ENU) would be contacted and it would forward the request.- the ELO would consult EUROPOL's Information System (EIS) and the Analytic Work Files (AWF).
- Direct access to EUROPOL's EIS via the secure communication IT network using SIENA.
- Direct information of MS B and MS C via EUROPOL's secure email system and the SIENA messaging service application
- Direct secure messaging from the National INTERPOL Bureau (NCB) in MS A to the NCB in MS B.
- Secure messaging to INTERPOL General Secretariat, Lyon, (IPGS) via the National Bureau (NCB). IPGS does not accept requests other than from an NCB.
- Access to IPGS databases via ASF mail or direct access.
- In case of SIRENE to SIRENE communication the IT network SISNET is used to exchange secure emails largely based on standardised forms.

Most MS indicate that further cross-border exchange will depend on the responses of EUROPOL, INTERPOL, MS B and MS C. If there were positive results, some MS would send an INTERPOL ST Message to Zone 2 countries with special attention to MS B and MS C informing them about the results obtained.

However, there are a few peculiarities. Some may be caused by legal reasons and others by the fuzziness of the responses, but some may be worth summarising for later discussions with and among MS.

- Not all authorities would contact EUROPOL; in particular EUROPOL's capabilities (Phoenix AWF) are not stated, even not by those who would involve EUROPOL and those MS actually using the EUROPOL channel do not clearly explain how they would achieve this but just say that they would co-operate with EUROPOL - therefore, the level of technical implementation remains unclear in many cases.
- Not all MS using the INTERPOL channel, either exclusively or simultaneously, indicate if the Zone 2 Message would be sent to all MS or if it would only be a 'diffusion Zone 2 except Schengen'; other MS indicate that they would contact INTERPOL to gather additional information without specifying any more details and as is the case with the EUROPOL channel, the grade of the deployment to users is indistinct
- Some MS would start the initial co-operation via liaison officers rather than using European-wide services.

Case study 2:
A law enforcement officer has confiscated 500 grammes of heroin during a routine check of a suspicious person and found on the bags a tuft of hair not belonging to that person. In addition, he has seized a mobile phone, which the individual is suspected to have used to make calls related to the smuggling operation. There are also signs that the car the person was driving had been stolen. The agent suspects that that this person is a member of an organised crime group involved in car theft and drug trafficking that may be active in several EU Member States.

Basically, the answers to this hypothetic case do not much differ from those in case study 1. In addition, the seizure of the mobile phone was taken into account by most MS. Although Prüm is not fully implemented, MS who are legally and technically ready stated that they would analyse the hair tuft and send the DNA profile to other countries. Even many of those who are not yet ready for Prüm would send the analysis via other channels than the automated Prüm search request.

It was often highlighted that for gaining subscriber details of the phone numbers stored in the phone, legal assistance would be required, which would be likely to slow down the procedure. The quantity of drugs – 500 grammes -was not always considered significant.

In contrast to case study 1, EUROPOL was the first choice, not necessarily excluding the use of other channels such as INTERPOL, LEA specialised cross-border networks or bilateral contacts. A check in the SIS partly stated that the search in the INTERPOL stolen vehicle database would clarify the status of the car.

Points to emphasize:

- The main problem here is the different legal systems (rogatory letters), especially for gathering the phone subscriber details.
- Time delays regarding responses to requests are a large concern.
- Although database searches to find out if the car was stolen are often mentioned, only one MS mentions the consultation of EUCARIS (EUropean CAR and driving licence Information System) for gaining the car owner’s details - the car could have been stolen very recently and not yet stored in the international wanted vehicle databases.

Case study 3:
A bank in your country has reported to your agency that several bank clients had received and replied to emails asking them to enter their details on a fake web site that closely resembled the legitimate one. Several bank clients in your country suffered financial damage, as criminals stole their usernames, passwords, credit card details and took that information to withdraw money from their bank accounts. During the investigation, your agency discovers that the criminals set up the scam site in Member State "B", but transferred the money to bank accounts in Member State "C".

Apparently, this was the most difficult case to answer. Many authorities said that they would use the EUROPOL channel and some even mentioned EUROPOL's Cyborg AWF.

Nevertheless, there are quite a number of authorities who did not answer at all. Those responding to this question gave partly vague descriptions. The given information about actions ranges from contacting EUROPOL to notifying emergency contacts via secure SMS. A few authorities indicated that they have a national cyber crime department which would be informed and take further action. Finally, several parties had doubts that the case study reflects reality. Usually, cyber crime was committed from outside the EU where criminals are less at risk of being caught.

Similar to case study 2, concerns have been raised about delays when rogatory letters are required. Further difficulties are experienced when cases call for immediate action outside office hours.

There was a common understanding that any means are useful in preventing further damage. The reported channels are:

- EUROPOL
- INTERPOL
- 24/7 service in MS B (without mentioning who this would be)
- Liaison officer in the MS concerned
- The FIU representative in MS A via FIU.NET
- CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team)[36]
- The ISP directly
- The bank or financial institution directly
- Any useful channel

Main findings:

- A coherent procedure does not exist
- Any channel and any IT and communication tool may be useful
- Legal assistance procedures cause the risk of delayed action

[36] http://www.enisa.europa.eu/act/cert/background/cert-factsheet

4 Common obstacles hampering efficient cross-border information exchange

From the general point of view, the exchange of information and criminal intelligence with the EU MS is functioning reasonably well. Nevertheless, almost all MS see room for significant enhancements, particularly by ensuring that procedures for spontaneous exchange of information are improved in the future. In addition, the existing instruments should be consolidated and actually used as originally envisaged. According to some MS, EUROPOL could be used in a better way because it is sometimes seen to be unclear what kind of criminal intelligence can be provided to EUROPOL or made available by them. In some (old) EU MS different national barriers also hinder efficient and effective cross-border information exchange. For example, the different locations of services or weak national co-ordination and communication within the country hamper cross-border information exchanges. The effectiveness of such exchanges therefore needs to be considered alongside the effectiveness of internal exchanges.

Trust can be regarded as the most important factor in the process of cross-border information exchange and the greatest enemy of trust is corruption or the fear of corruption. Perhaps surprisingly, almost all MS stated that they trust other MS, which does have a positive impact on cross-border information exchange within the EU. It can be assumed that even greater trust between different MSs could be achieved by a limited number of SPOC and staff consistency. This would enable representatives of different states to create better personal relations.

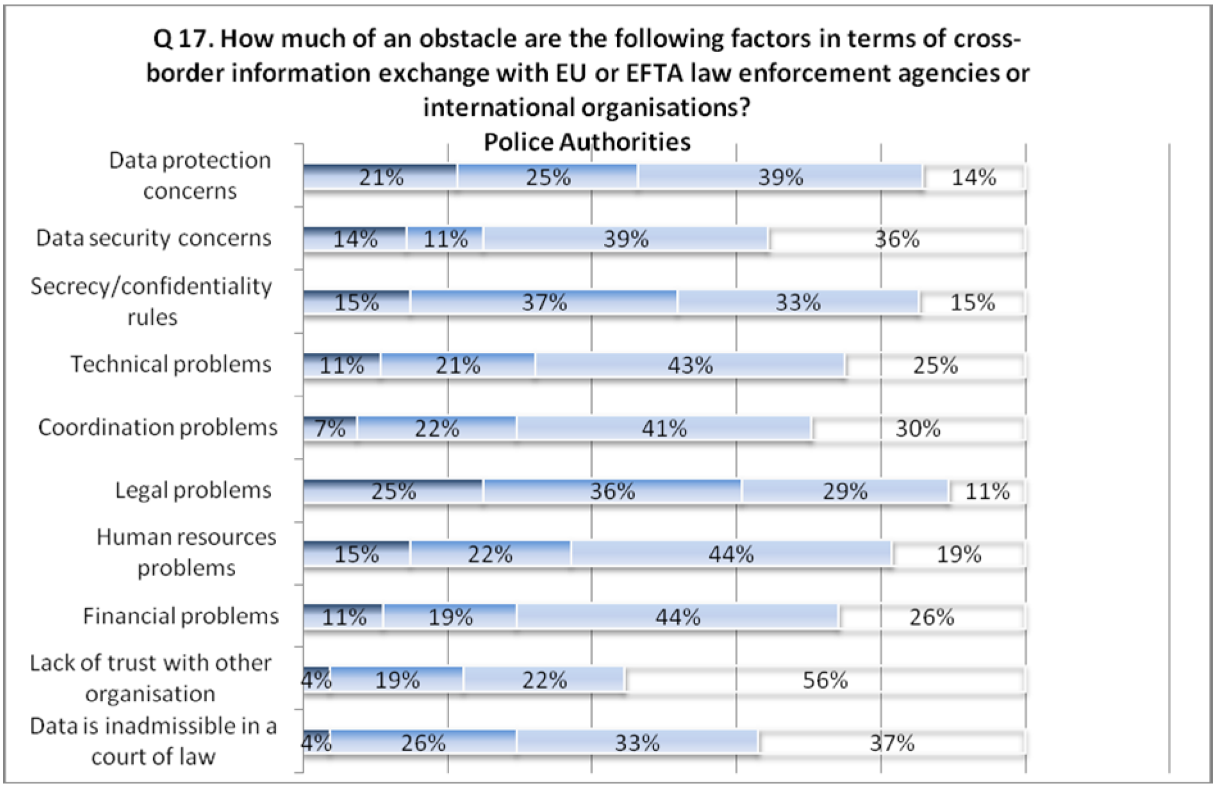
While EU MS LEA's largely trust each other, distrust within some MS among their national authorities definitely hamper efficient cross-border information exchange. There was even a case when one national authority was not ready to provide information to the International organisations because other domestic organisation would then have access to this information. Though the trust and co-operation between INTERPOL and EUROPOL is on a high level, this is not the case in some MS where mistrust between ENU and NCB does take place. However, in most cases EU MS LEA's trust other organisations to handle data according to the same data protection and security standards.

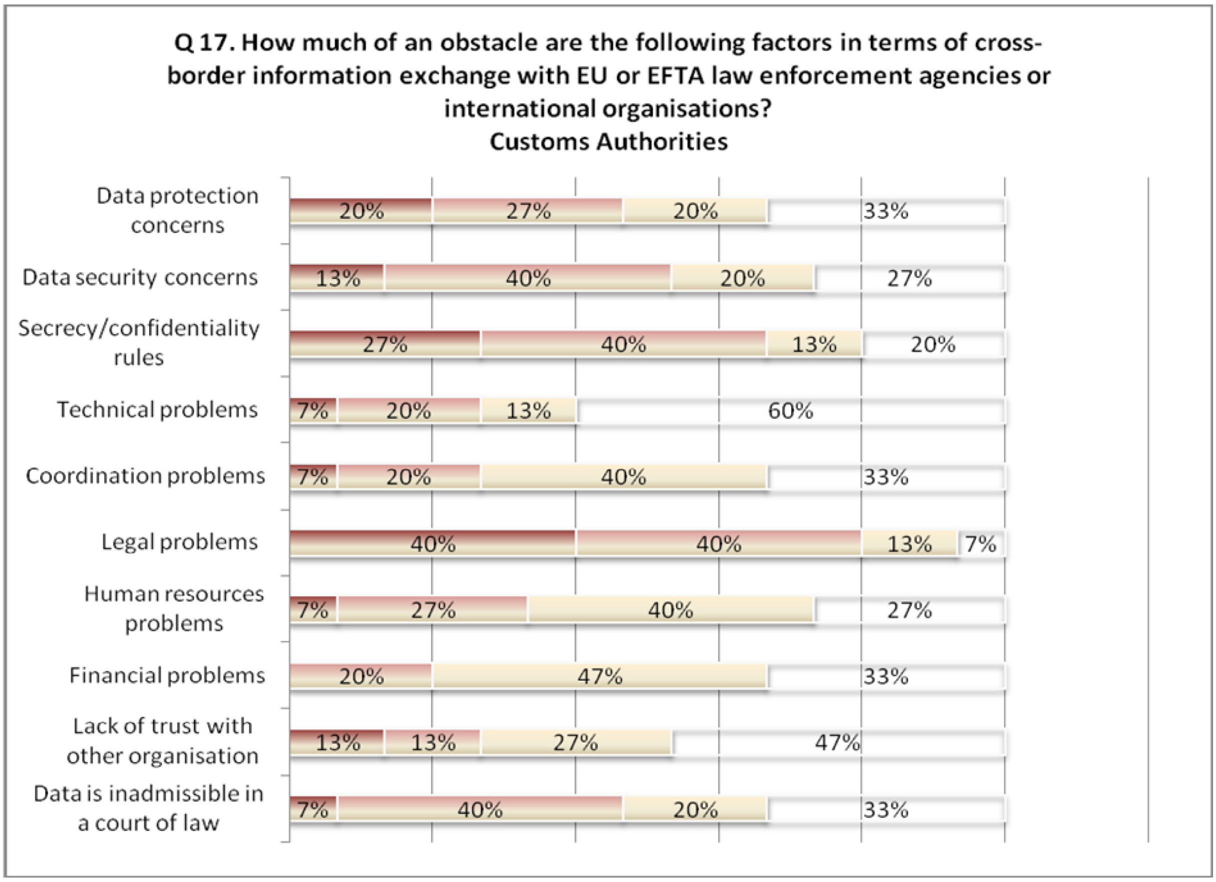
The answers to the questionnaire provided by MS and detailed in the graphs produced below and at the end of this section reveal that the existing practices of cross border information exchange do add value to the results of LEA's daily work. Linguistic barriers do exist to some extent but do not have a very significant effect on the cross border information exchange. As pointed out by several MS, one common language (English) for urgent requests would certainly improve the responsiveness of LEAs and facilitate the exchange of information. Furthermore, law enforcement authorities do not generally have major problems with identification of the appropriate counterparts in other MS because the centralised authorities in other MS are responsible for dispatching requests to their authorized units. However, a significant number of MS did have problems here and, although these difficulties were not great, they felt that good practice would be the receiving state's agency always ensuring that requests were forwarded on, rather than returned. The national legal environments are diverse and they do affect cross border information exchange. MS LEAs seldom experience IT problems within their MS which cannot be overcome quickly. Normally, MS LEAs do not lack proper IT facilities to manage cross border data exchange and sufficient IT support is available. Nevertheless, the existent different IT systems certainly make it difficult to achieve interoperability and lack of secure email systems is an issue for some MS (e.g. UK). Surprisingly large proportions of exchanges are done by fax or postal mail, partly for this reason.

Lack of staff is evident in some (old) EU MS while in some other (new) EU MS this is not so obvious. The fact is that Prüm has added new commitments and increased the workload, especially when new partners join, the hits are numerous at the beginning. Although cross-border exchange has increased, only in a few EU MS have the staff increased in correlation to the growth of cross border information. EU MS LEA's mostly relay information via technical communication channels, although some MS exchange sensitive data only via liaison officers. To conclude, the currently available EU instruments broadly correspond to the LEA's operational needs, but the resources backing them up are increasingly stretched.

The results of the analysis show that the main problems in cross-border information exchanges are legal problems, especially data protection legislation, followed by secrecy and confidentiality problems. Details on the legal problems highlighted by the MS can be found in chapter 4.1.

Table 8: Perceived obstacles to information exchange between EU MS and with EFTA countries – Police Authorities and Customs Authorities (read left to right: major obstacle to no obstacle)



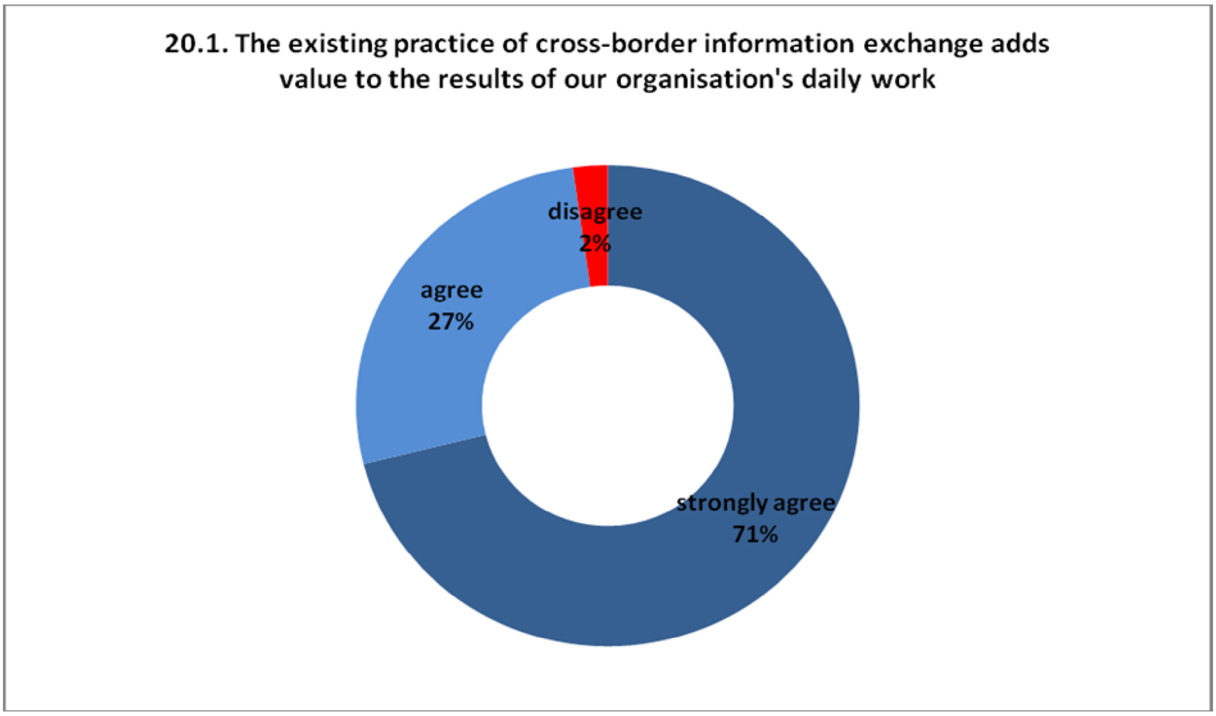

Q 17. How much of an obstacle are the following factors in terms of cross-border information exchange with EU or EFTA law enforcement agencies or international organisations?
Customs Authorities

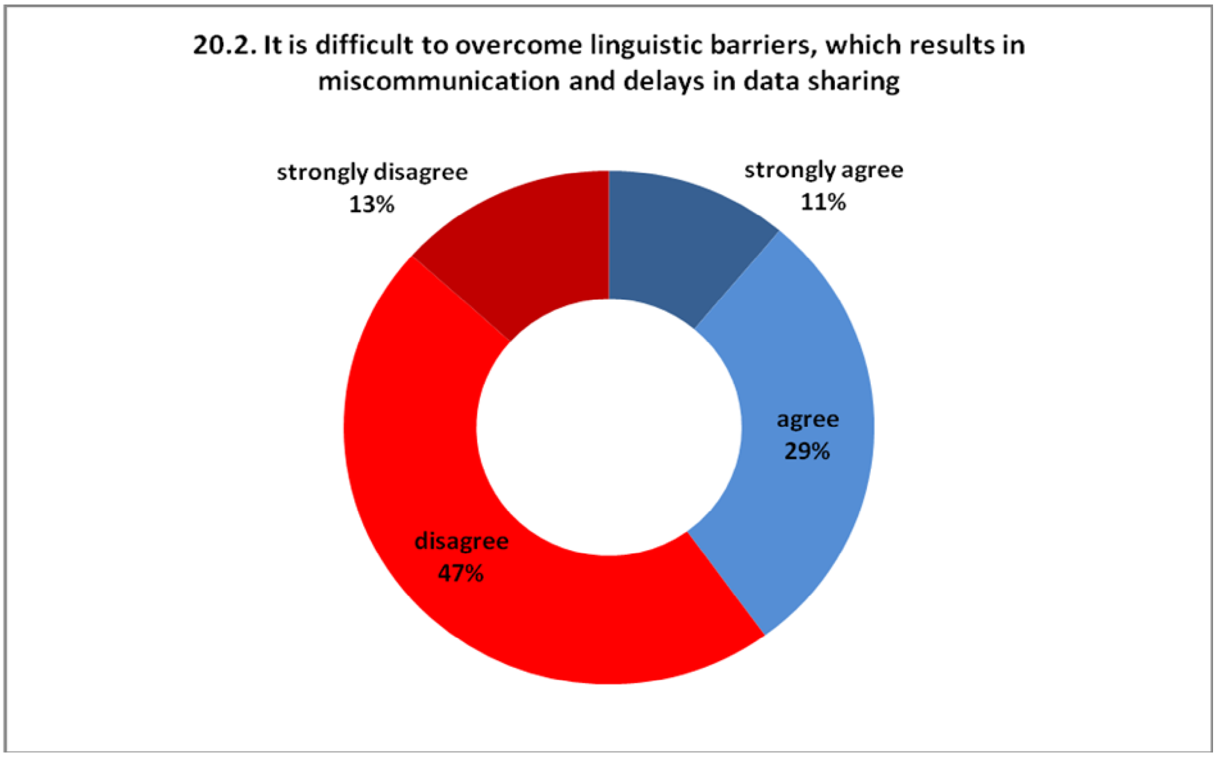
The following additional obstacles were identified in the course of the Study research and pointed out by the EU MS:

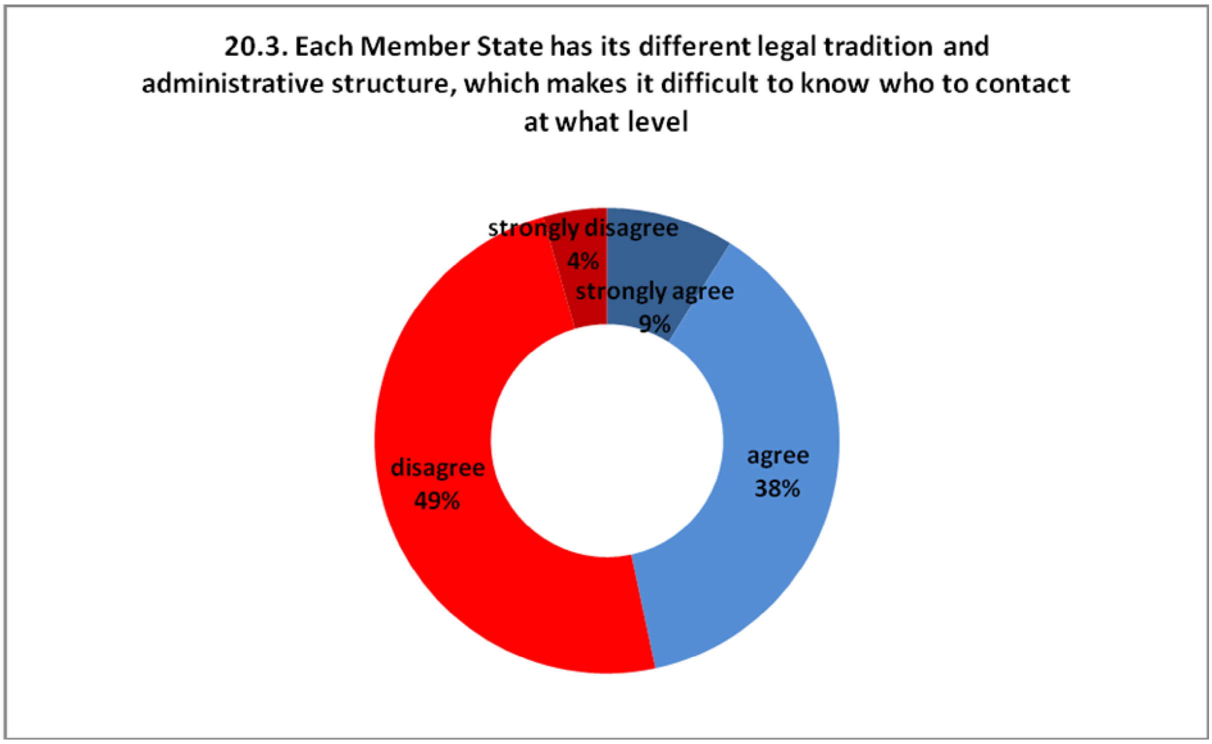
- signed and but not ratified agreements on police co-operation hinder efficient cross-border information exchange
- vagueness of what type of information other MS can provide to the requesting MS
- lack of 24/7 Single Points of Contact and 24/7 National EUROPOL Units
- failure to give reasons for a request and/or reasons why a request is urgent

Member States very clearly pointed out difficulties with telecommunication data such as subscriber's details (particularly mobile, prepaid and other), phone calls, etc. which are one of the most needed and requested pieces of information for law enforcement authorities. However, different national legal systems hinder access to national providers and consequently hamper efficient cross-border exchange of these kinds of information. For example, in some EU MS these kinds of data can be easily obtained from private companies while in other countries they are not freely available or are only accessible with prior judicial approval, and judges demand justification of the need for this information before the requested data is to be made available Moreover, in the United Kingdom private companies require compensation from Law Enforcement Authorities when providing such types of data.

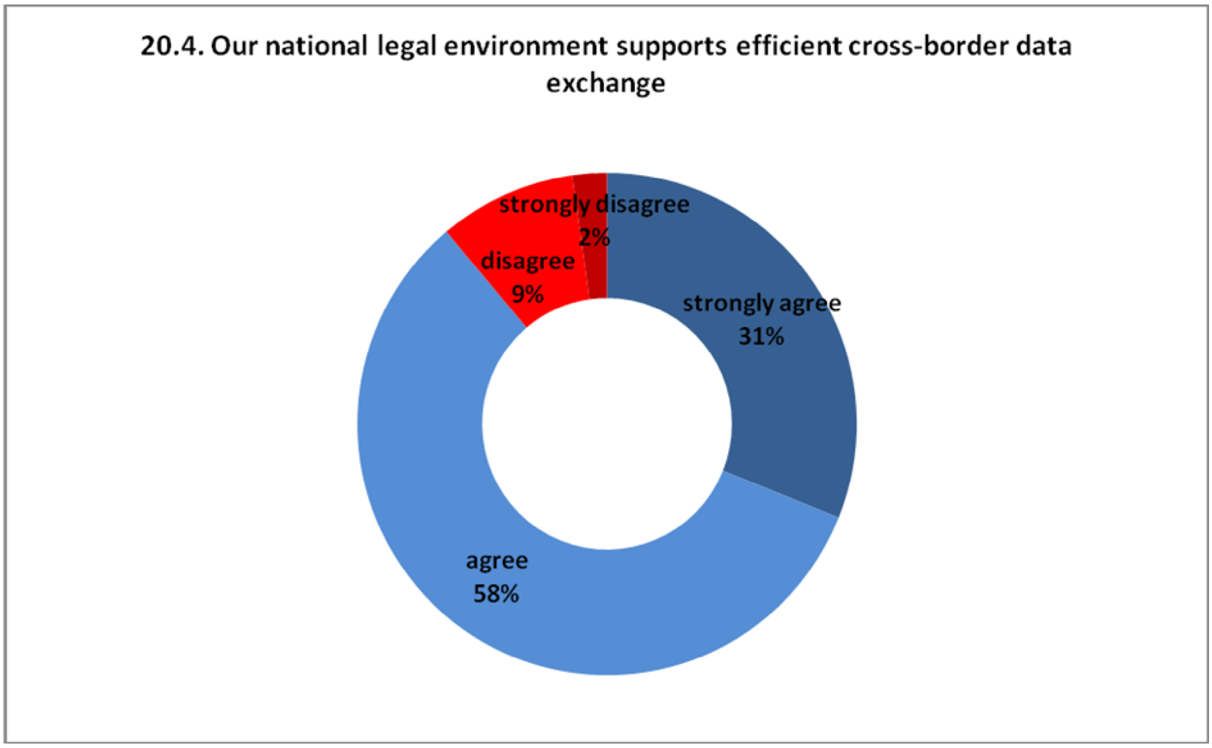
The presence of a vast number of different databases/registers in EU MS prevents an efficient exchange of information also. It should be noted that in some EU MS there are several police forces (aside from other law enforcement agencies with full investigatory authority), all of which have different policing systems, distinct databases and registers, different legal bases and legal authorizations, etc. The example of the Italian and French P(C)CCs, which have access to 65 databases or registers dramatically demonstrates this. Frequently personnel dealing with cross-border information exchange do not have access to information at all, or in an inappropriate timeframe, which results in information and intelligence not being exchanged, despite a will to do so. To overcome this fragmentation, personnel at central level should have access to all relevant information and intelligence, or at least to administrative registers indicating whether and where further details are held and which agency has "lead" responsibility.



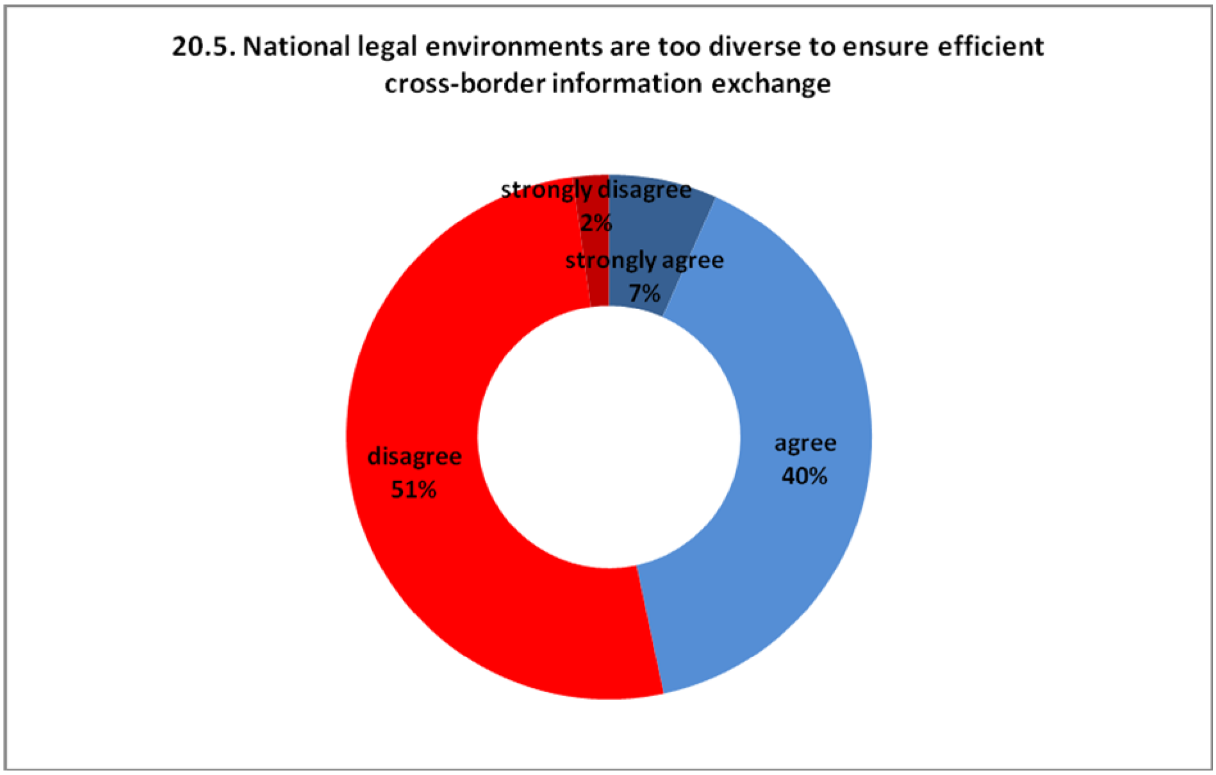


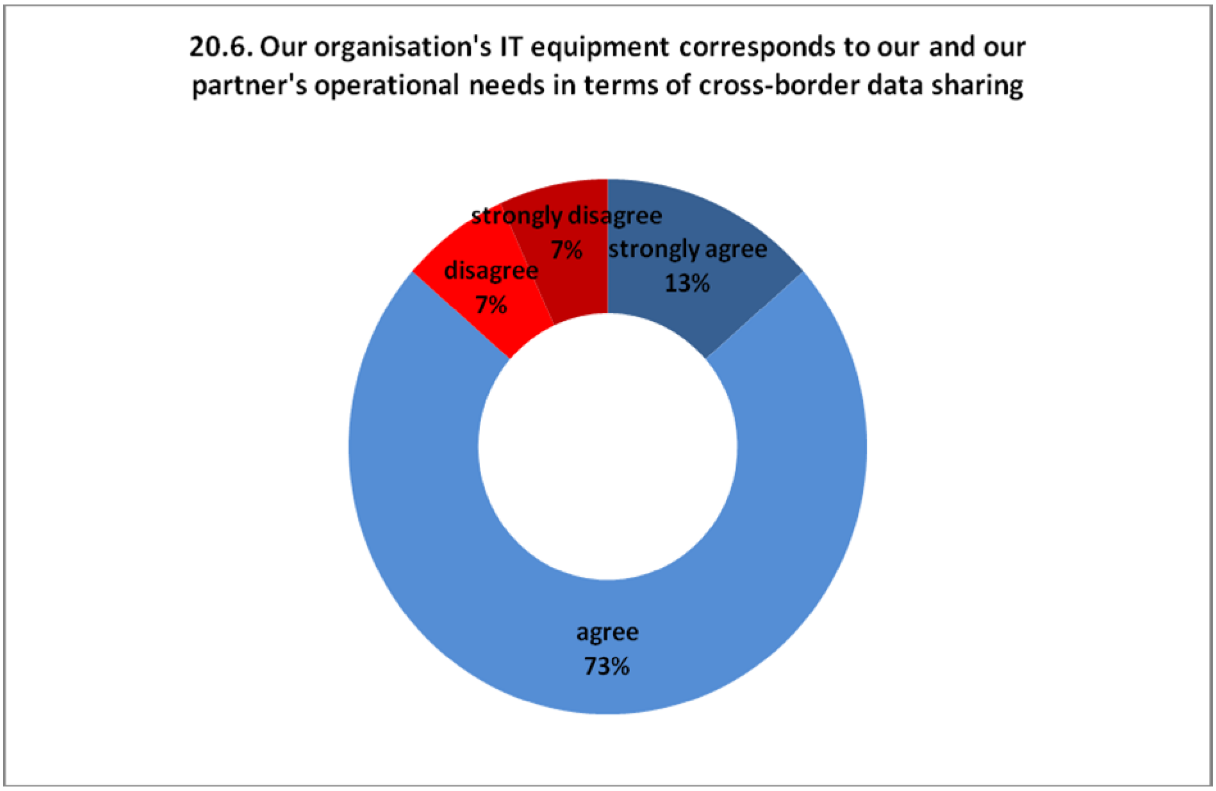


20.3. Each Member State has its different legal tradition and administrative structure, which makes it difficult to know who to contact at what level

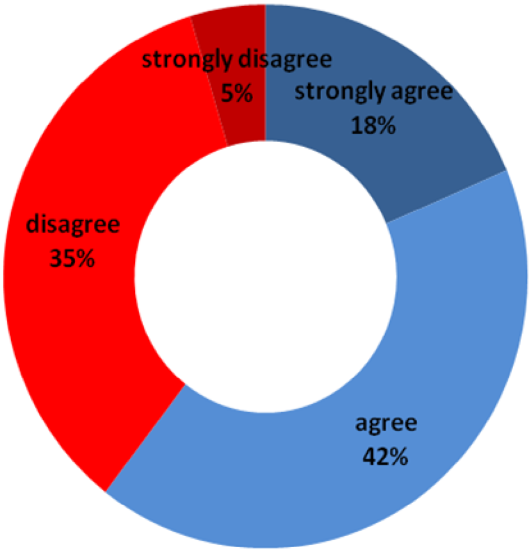


20.4. Our national legal environment supports efficient cross-border data exchange

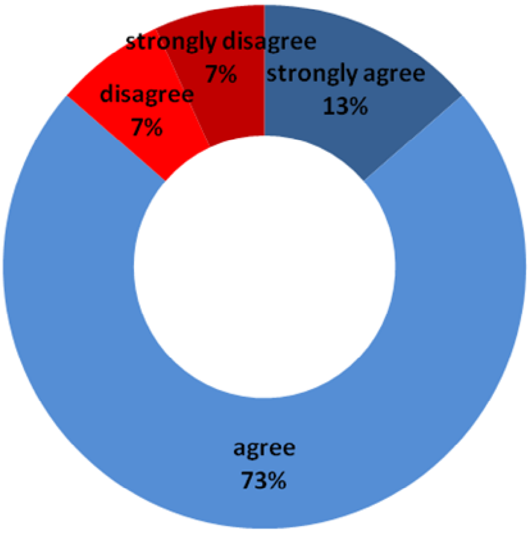

20.5. National legal environments are too diverse to ensure efficient cross-border information exchange
strongly disagree
2%
strongly agree
7%
agree
40%
disagree
51%

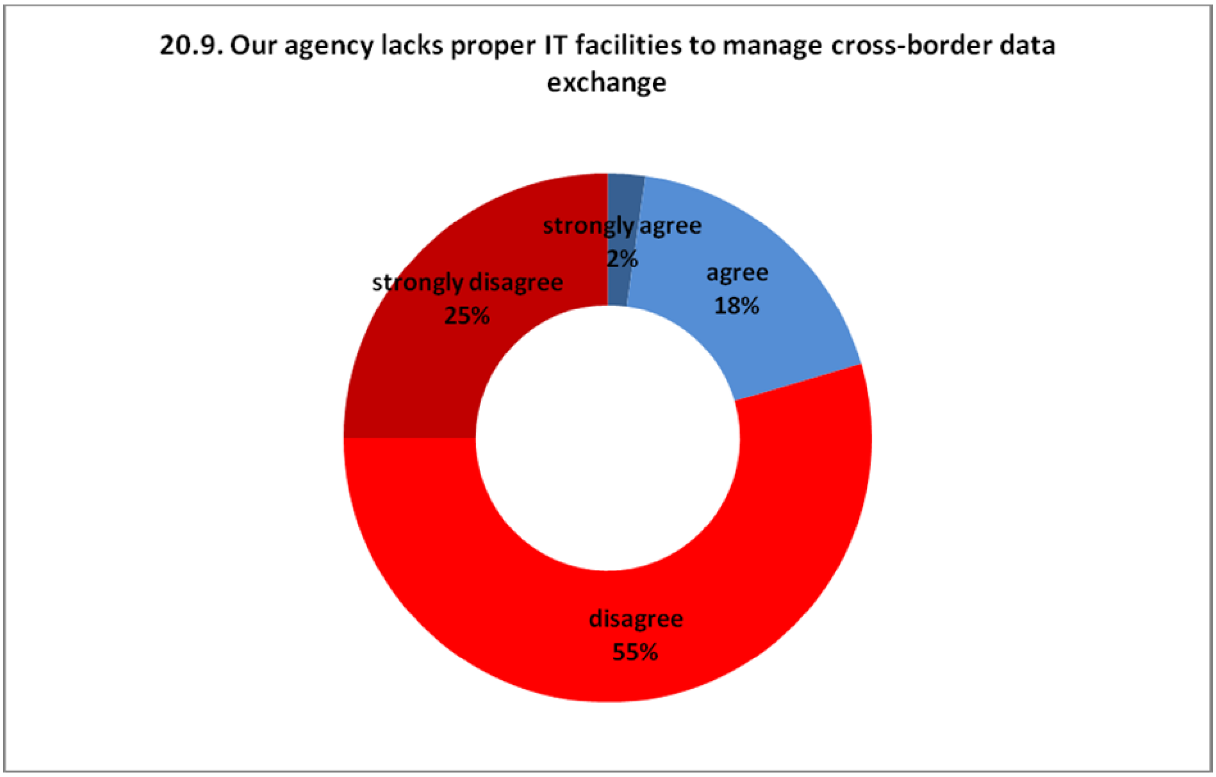

20.6. Our organisation's IT equipment corresponds to our and our partner's operational needs in terms of cross-border data sharing
strongly disagree
7%
strongly agree
13%
disagree
7%
agree
73%

20.7. Each member state has its own IT system, which makes interoperability difficult to achieve

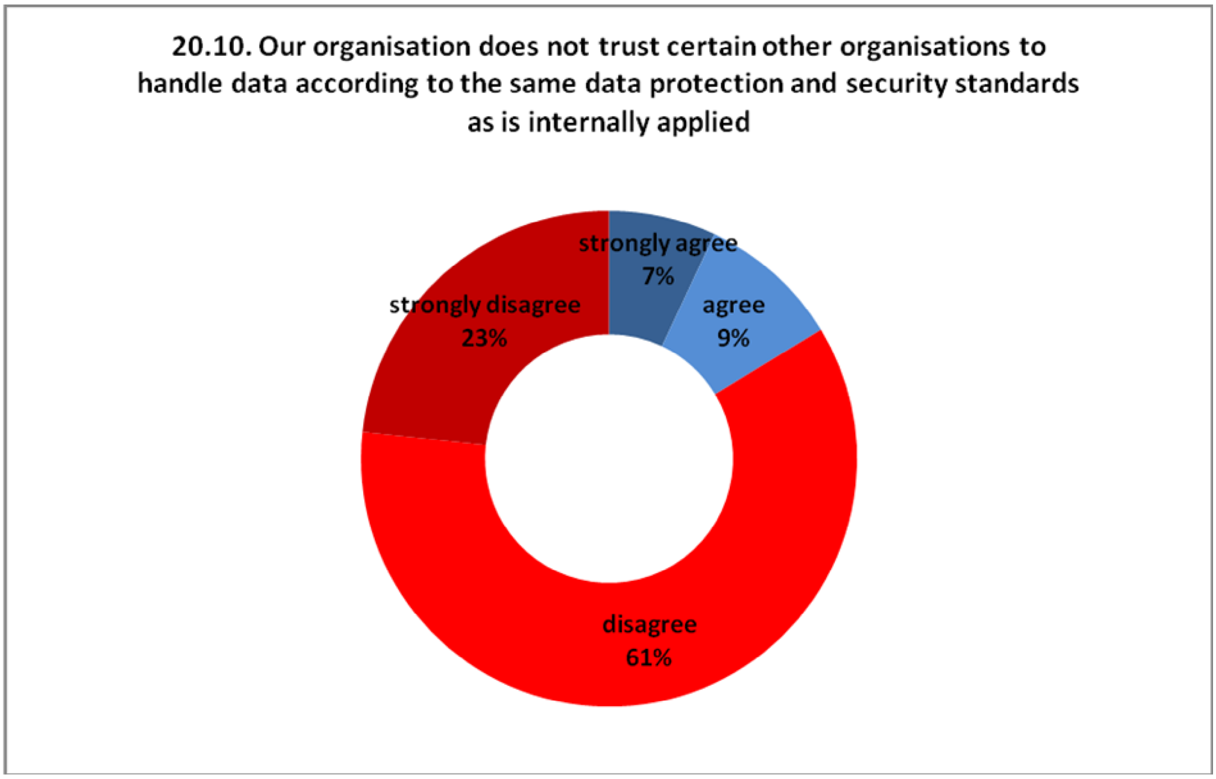


20.8. Our organisation seldom experiences IT problems which cannot be overcome quickly and sufficient IT support is available

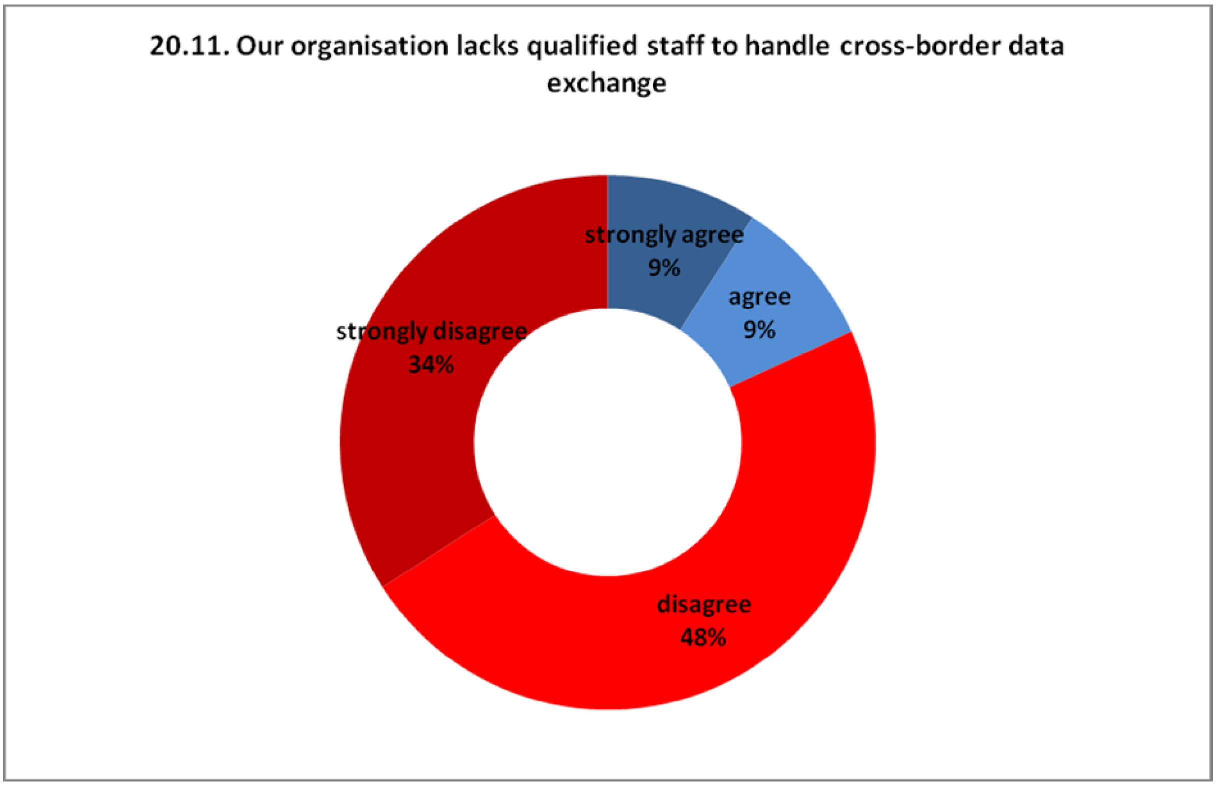




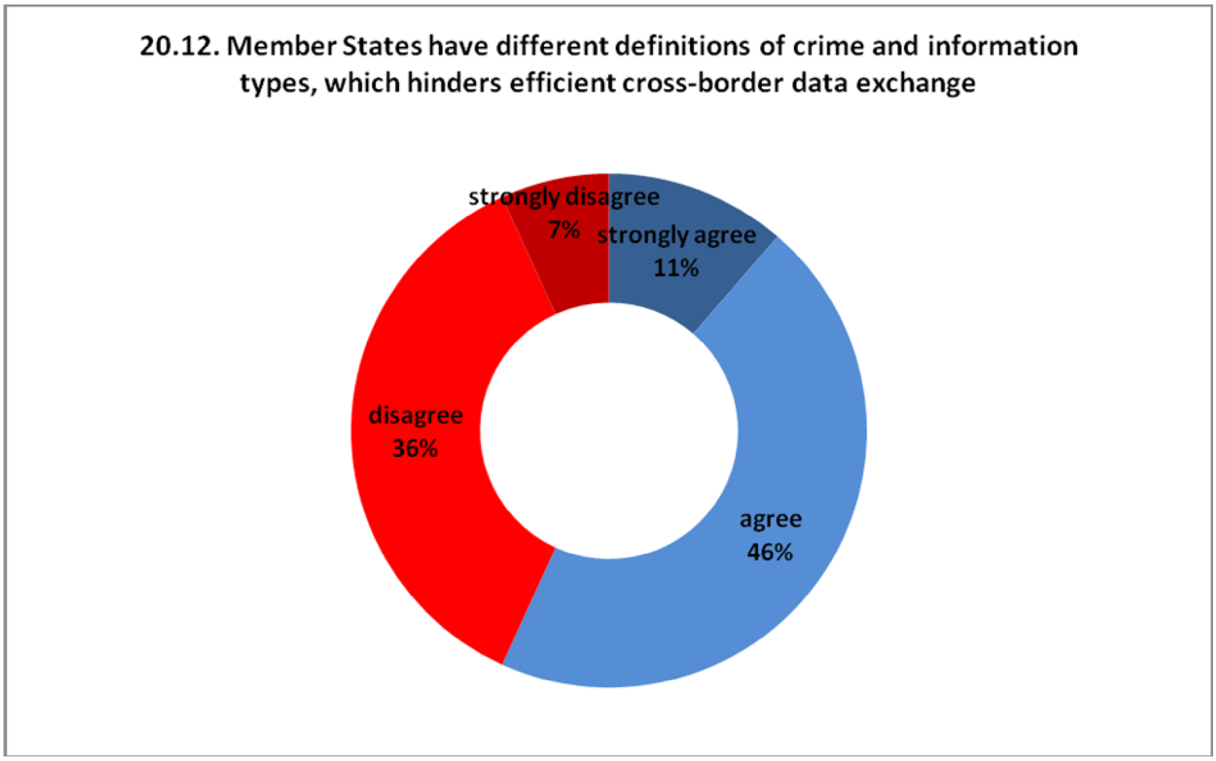
20.9. Our agency lacks proper IT facilities to manage cross-border data exchange



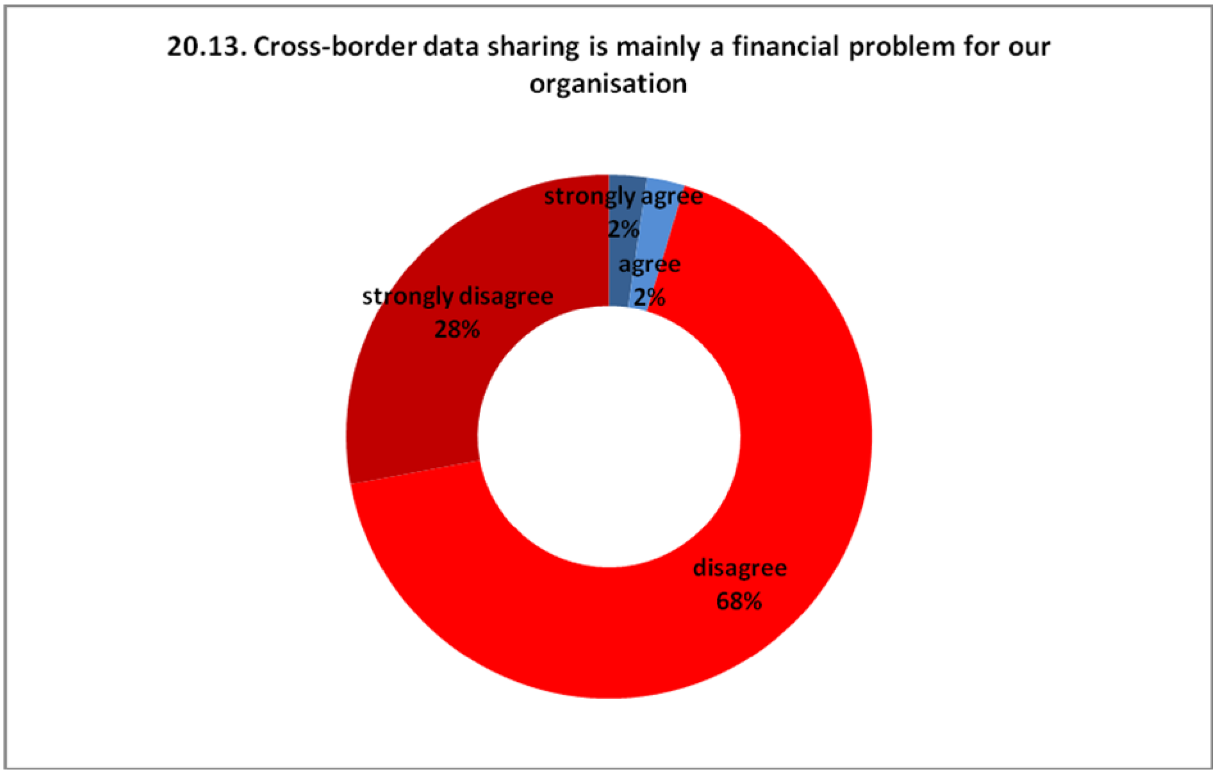
20.10. Our organisation does not trust certain other organisations to handle data according to the same data protection and security standards as is internally applied

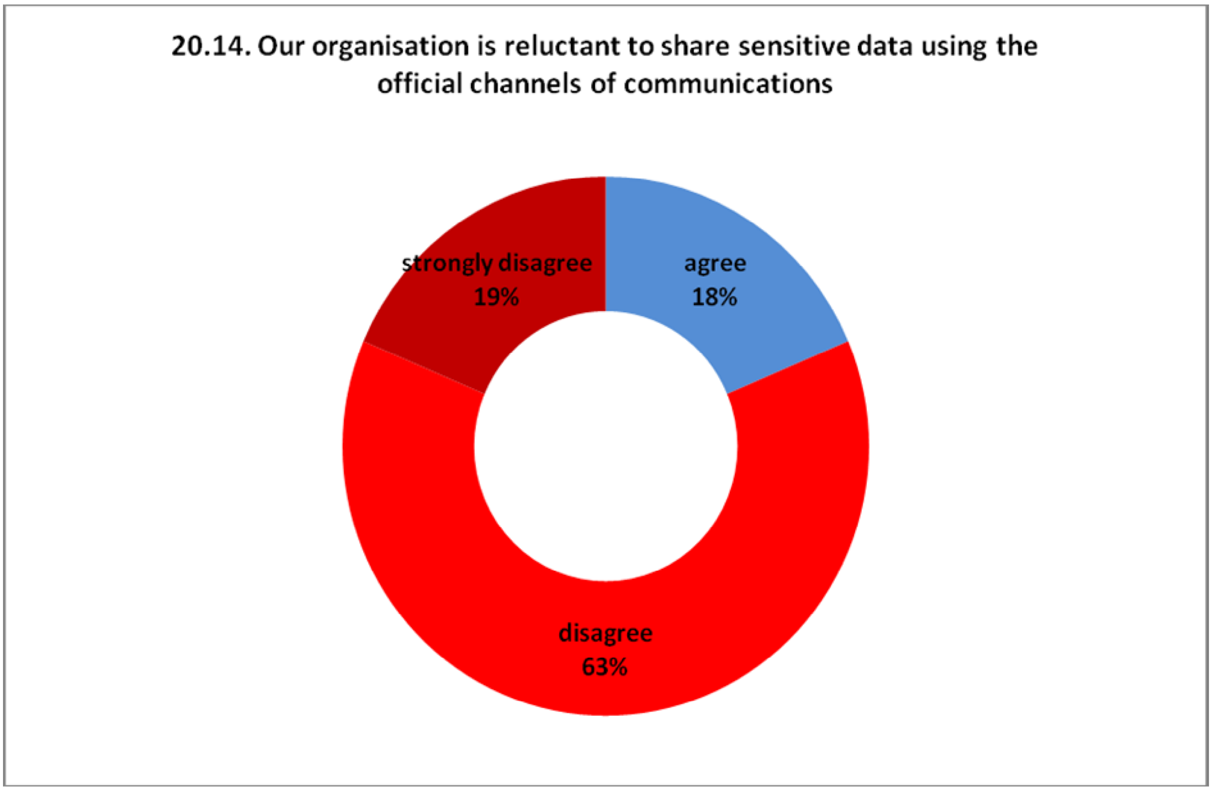


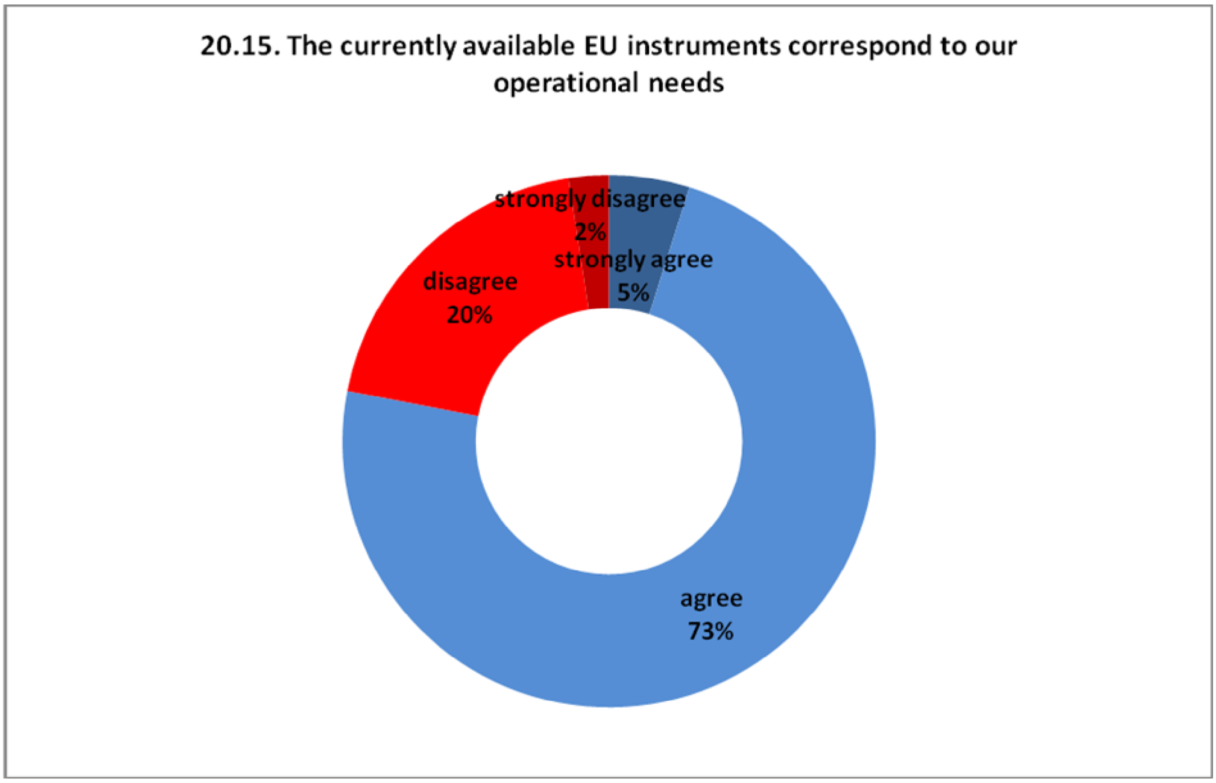
20.11. Our organisation lacks qualified staff to handle cross-border data exchange



20.12. Member States have different definitions of crime and information types, which hinders efficient cross-border data exchange


20.13. Cross-border data sharing is mainly a financial problem for our organisation
strongly agree 2%
agree 2%
strongly disagree 28%
disagree 68%


20.14. Our organisation is reluctant to share sensitive data using the official channels of communications
strongly disagree 19%
agree 18%
disagree 63%



20.15. The currently available EU instruments correspond to our operational needs

4.1 Legal problems

The requirements of different national legal systems definitely hinder efficient and expeditious law enforcement agency co-operation, and the differences mainly relate to differing interpretations in MS as to when a Rogatory Letter is required. Sometimes Rogatory Letters are also required for certain types of crime (e.g. economic crimes) which, according to some MS, could be exchanged through the police communication channels. In some cases Ministries of Justice are responsible for information disclosure for certain categories of data usually required for police work, and this consequently requires judicial involvement (e.g. DNA related information is under the Ministry of Justice in the Netherlands). Such situations, according to all interviewed MS, certainly hinder or at least slow down significantly cross-border information exchange and, finally, this situation is not in accordance with the Principle of Availability. In order to address this problem an agreement between MS might be considered; that in cases when certain information can be acquired in the requested state only with prior court permission the LEA drafting the request should acquire beforehand analogous permission from its national court to obtain such information. This is the procedure of drafting Rogatory Letters. Therefore the application of an analogous practice could be possible in the exchange of information through existing channels also. The Guidelines on the implementation of the Swedish Framework Decision do provide detailed information on the categories of information that could be obtained from a particular MS only if prior permission from a court is available. This would also avoid formal legal obstructions when acquiring information through the discussed channels of information exchange. According to some MS, clarification could also be brought by way of a new EU legal act.

Moreover, traditional MLA instruments do not always ensure the speedy execution of request. Some of the problems detected are related to delays in the execution of Rogatory Letters, and subsequent requests for supplementary information. The limited use of mutual recognition instruments, partly because they have not been implemented under national law by all Member States, also requires early and serious consideration, while naturally appropriate legal safeguards need to be ensured.

According to some MS, one of the key legal problems relate to sharing of classified (confidential) information. When confidential information is received, it is very difficult to share it with other MS or sometimes other agencies in the receiving MS and only a narrow range of authorized persons have access to that information.

The existence of different national (internal) classifications in MS regarding the same types of data significantly hinders the effectiveness of cross-border information exchanges. A clear example of this is the significant amount of criminal investigation and criminal intelligence information exchanged by postal mail as the security of electronic systems is deemed insufficient. Harmonization and detailed clarification of the classification of data types would, according to some MS, improve considerably cross-border information exchanges (e.g. what types of data should be classified and to what level, i.e. an indicative system, issued with recommendations explaining the identical, similar and different definitions within MS).

Some MS reported that different wordings and understandings of (EU) legal bases cause legal and practical problems in the implementation process. The same legal texts can be quite differently understood, interpreted and consequently implemented in different Member States. For example, expressions used in the French, Dutch or German version of the Schengen Convention do not correspond to expressions used in the law of the country where the language concerned is an official language[37]. Consequently, different versions of the same EU legal act do not correspond with one another and may be interpreted differently. Therefore common guidelines on the implementation of legal instruments should be adopted wherever possible.

UK Customs (HMRC) differs from other MS in its interpretation of the legal channels which can be used for the application of coercive measures, i.e. compelling persons to provide information to assist enquiries requested by another MS. The UK does not accept that Naples II overrides national legislation in this respect, and holds therefore that Naples II does not authorize the use of coercive measures to gather information in the UK. It holds that MLA procedures, i.e. Rogatory Letters, must be used. The UK (HMRC in this case) notifies the requesting country that the request cannot be proceeded with under Naples II and that Mutual Legal Assistance judicial procedures must be followed. The UK does not, of course, refuse the request outright. The introduction of the European Investigation Order (EIO) will probably clarify and simplify the execution of measures in the UK as the EIO implicitly and explicitly recognises that the executing state will need to use coercive measures.[38]

Germany and Finland have pointed out that there needs to be greater awareness within police forces in MS where they are tasked with investigations of Customs matters, of the role of OLAF and the distinctions between the uses of the Naples II procedures for First and Third Pillar matters. The First Pillar covers exchanges in relation to prevention and detection of threats to Community customs legislation and therefore the Community budget, whereas the Third Pillar covers such measures against national MS legislation (e.g. drugs and counterfeit goods smuggling) and the prosecution by MS of offences against Community legislation and the Community budget.

Generally speaking, the main legal problems in cross-border information exchange derive from the differences in national legislation in MS. Several MS pointed out that a lack of harmonization of different national legislations can cause, and has caused, massive discrepancies in the actual use of EU legislation. For example, different criminal laws define different law enforcement procedures in cross-border information exchanges. In some EU MS Rogatory Letters are required for certain types of data (e.g. DNA) while in other EU MS this is not the case. Also, different privacy and data protection laws differently regulate law enforcement access to the same type of data: For example, phone subscribers' details accessible to law enforcement authorities in one MS may not be accessible to law enforcement authorities in some other EU countries without judicial permission providing a necessary check and balance to unfettered actions of the state. Furthermore, a few EU MS have entered several thousand alerts of article 99 SIS while other states have entered very few or none[39] and similarly for article 96 SIS (persons to be refused entry to the Schengen area). The discrepancy can be explained by the

[37] Schengen Investigated, A comparative Interpretation of the Schengen Provision on International Police Co-operation in the light of the European Convention on Human Rights; Chantal Joubert & Hans Bevers; page 11

[38] see paras. 10 and 11. of the preamble to the Council of the European Union's document 9145/10 of 29th April 2010: Initiative for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters

[39] On 01.09.10 there were approx 35 000 Article 99 alerts in the SIS, 17 000 of them being French and 9 000 being Italian.

divergent interpretation and implementation of the SIS rules in the EU MS, but is nonetheless a matter of concern.

Criminal proceedings in each MS are regulated by different national legislation, thus even though the main principles are the same, the specific provisions related to the application or the scope of the data are rather different. As criminal proceedings matters are fundamental to national sovereignty, awareness of each other's procedures needs to be widely circulated and understood.

According to EUROJUST legal obstacles are clearly related to differences in criminal procedure and evidence. Examples can be found in different legislation regarding interception of communications, the hearing of witnesses, the degree of witness protection available (e.g. in cases involving organized crime or trafficking in human beings), and fair trial requirements in matters of evidence (e.g. witness statements being admissible only when taken before a judge, but not when taken by the police). When examining some principal judicial co-operation instruments (letters rogatory/MLA, transfer of proceedings, recognition of decisions/judgments, and extraditions/EAW), EUROJUST noted the following specific legal difficulties in operational cases:

- the potential inadmissibility of evidence obtained by Rogatory Letter when the standards or legal requirements for evidence-gathering in the issuing State are different from those in the requested State;
- despite provisions in the 2000 MLA Convention[40], failure by the executing Member State to meet the formalities and procedures requested by an issuing Member State;
- delay in the ratification of instruments: problems have been identified in setting up a JIT, in applying the Convention on Transfer of Proceedings and in the use of interception of telecommunications[41].

It remains the case after 10 years that the 2000 MLA Convention has still not been ratified and implemented by all MS and this lack of implementation may cause some delays during the handling of the case because different solutions must be found. For example, in a case mentioned in the EUROJUST Annual Report, one Member State refused to transfer the signal to carry out a direct interception to another Member State (possible according to extensive interpretation of the 1959 Convention as it is a mere technological problem) because the latter had not ratified the 2000 Convention. After intervention of EUROJUST, an EAW was issued and the interception could be finally executed. In a similar case with another Member State regarding a videoconference to hear a witness, the problem was solved thanks to the mediation action carried out by EUROJUST.

Following are further examples for differences in national legislation which lead to practical problems in cooperation. Varying legal requirements for the conduct of investigations and prosecutions may cause obstacles. For example, the presence of a lawyer during witness interviews conducted abroad may not be required in legal systems outside the European Union. It might follow that evidence or witness statements obtained without the presence of a defence counsel in, say, Turkey, may invalidate the use of the evidence in a national court of the

[40] Convention on Mutual Legal Assistance in Criminal Matters (2000 MLA Convention), 29 May 2000
[41] EUROJUST Annual Report 2009, http://www.eurojust.europa.eu/press_releases/annual_reports/2009/Annual_Report_2009_EN.pdf

European Union. To avoid delays or complications in the execution of these requests for MLA, legal formalities in different countries must be clearly outlined.

Controlled deliveries, JITs, and the interception of communications are co-operation tools frequently used in drug cases. Problems can arise due to the fact that controlled deliveries are subject in some MS to judicial co-operation, and in others to police co-operation. This situation can cause problems if the MS requesting assistance acts only on the basis of police co-operation without issuing an MLA request. In such cases, the requested MS, whose system for controlled deliveries requires judicial co-operation, cannot comply with a police request alone. EUROJUST frequently acts to provide solutions to difficulties of this type. In general, requests related to controlled deliveries have been executed swiftly. However, the transmission of police reports after execution has proved more problematic, especially in cases where police reports were categorized as classified information, a common occurrence in most MS.

Furthermore, following the principle of transparency in the Netherlands, a court must always have access to police information and a case history. As a result Netherlands Police cannot use information or intelligence sent from another MS if the sending MS has not approved t the information to be used for court purposes. If a sending authority in another MS refuses judicial use in the Netherlands (e.g. there is still an ongoing investigation), the Dutch Police cannot process the received information or intelligence under the requirement ‘for police use only’.

4.2 Technical problems

The main question in relation to technical problems and possible technical solutions is whether the existing technical solutions for law enforcement business processes are designed to meet current and future needs, as well as being open to expansion and modification in relation to the Principle of Availability. The need for enhanced co-ordination and coherence is clear. Member States indicated that there is a need to ensure that upcoming solutions consider LEA’s demands and that interoperability remains the biggest challenge for the future.

In view of a detailed questionnaire by the European Commission on technological issues in the framework of ‘Mapping 4’ of the Information Mapping Project, this study reflects only some IT details as far as they have been made available by the MS in the course of this study.

Specifically, MS indicated that a few of the current incompatibility issues were:

- Software versioning (i.e. MS or MS agencies are using the latest software versions, whereby attachments or documents, for instance, cannot be opened by the receiving party)
- Size of mails (in certain cases these exceed the technical capabilities of email accounts)
- Security rules (e.g. some countries refuse to accept certain emails or attachments)
- Different levels of technology available in the MS (ranging from fax to most modern web services)

According to EU MS, future technical solutions should be focused on:

- development of UMF (universal message formats)

- central availability of data in MS (including common cross agency databases, and/or central registries of basic information held in greater detail on other databases)
- bundling of information channels
- minimizing duplicated work and the replacement of it with single data input in different systems
- development of reliable automatic translation tools
- standardization that will not cause additional bureaucracy
- development of a "one web portal" allowing EU wide common searches
- consolidation, integration and interoperability of the existing IT systems
- introduction of cross-border encrypted video conferences

Further important points related to the coherence of IT channels and databases can be found in chapter 3.5.5.

4.3 Bottlenecks

Generally speaking, MS did not identify significant bottlenecks in the current procedures for cross-border information exchange. The need for translation can certainly be called a bottleneck in the handling of requests. A common bottleneck also occurs when a request is not within the competence of a receiving authority (as the competent authority in the receiving country may well be different from that in the requesting state). In these cases some authorities forward requests to competent authorities within their own country and notify the requesting authority about this transfer, while others invite the requesting authorities to resubmit requests to the competent authority.

Over-classification of information and intelligence often creates problems and can significantly disable further dissemination of information. This was pointed out both by several MS and by INTERPOL and EUROPOL. It seems that this more often happens in eastern countries where, for different reasons, (e.g. level of corruption) higher than normal classifications are required, with a resulting restricted access to the data. However, the Member State supplying information to EUROPOL is responsible for the choice of any appropriate classification level for such information. In choosing a classification level, Member States shall take account of the classification of the information under their national regulations, the need for operational flexibility required for EUROPOL to function adequately and the requirement that classification of law enforcement information should be the exception and that, if such information has to be classified, the lowest possible level should be assigned.[42]

According to EU MS, police exchange of information works quite well as long as Rogatory Letters are not required, as traditional MLA instruments do not always ensure the speedy execution of requests. Usually Ministries of Justice are the authorizers for the execution of MLA while in some EU MS Ministries of Interior and their police forces are responsible. Practical problems with the execution of MLA include the following[43]:

[42] Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of EUROPOL information (Official Journal L 332 , 17/12/2009 P. 0017 – 0022)

[43] EUROJUST Annual Report 2009, http://www.eurojust.europa.eu/press_annual_report_2009.htm

- lack of resources at national level for a timely execution of MLA requests or – following from the lack of resources – a "de-prioritisation" of MLA requests received from other Member States in favor of their "own" national proceedings;
- no acknowledgement of receipt of Rogatory Letters;
- difficulties arising from low-quality translations; or
- incomplete information included in MLA requests, especially where there is no reason given for the request.

The limited use of mutual recognition instruments, partly because they have not been implemented under national law by all MS, also requires consideration. EUROJUST is sometimes asked to intervene when these practical obstacles have not been resolved by use of the EJN.

National judicial authorities may lack experience of other criminal justice systems, of how assistance can be obtained most effectively and of why certain requests are formulated in a particular way. For instance, a procedural measure (such as formal questioning of a suspect) may be essential to prosecution in one MS but not another. A practical consequence of these different perceptions is that the execution of a request is given a low priority. The drafting of a thorough Handbook could help to solve this problem.

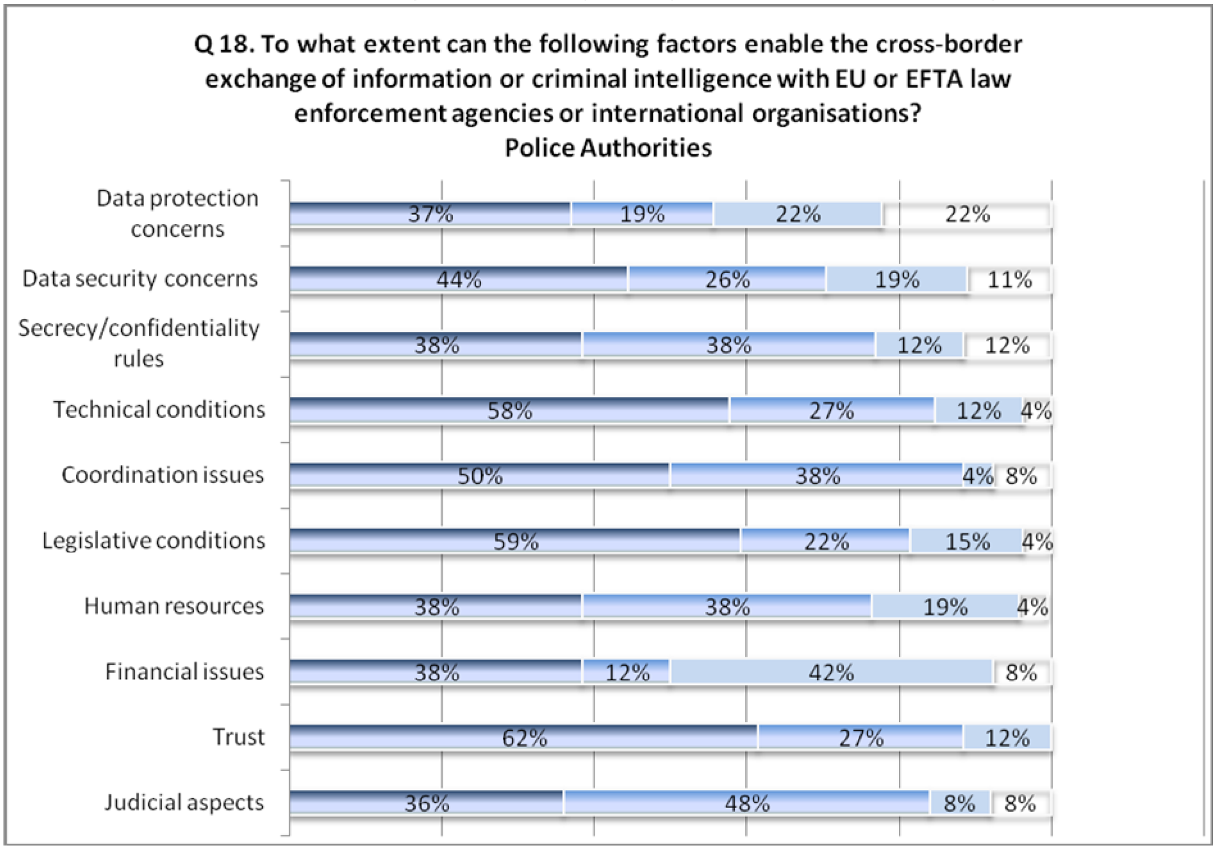
4.4 Redundancies

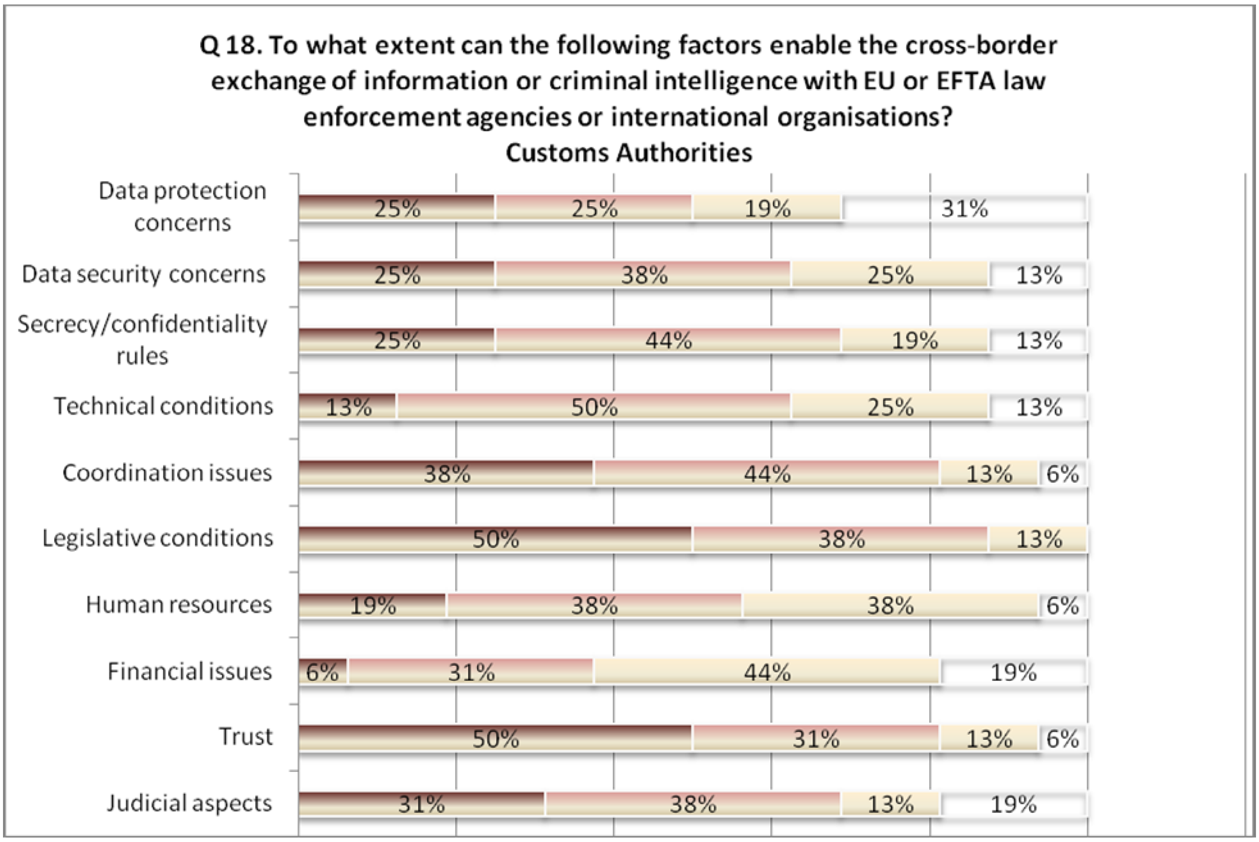
It sometimes occurs that MS send requests through two or three communication channels in order to be sure that their request will reach the correct recipients (e.g. because there is uncertainty in the requesting MS as to who has responsibility in the receiving state, or where several agencies in the receiving MS have responsibility depending on circumstances). Usually this does not present a big obstacle in MS due to generally efficient registration systems which normally detect such redundancies. In conclusion, such redundancies do not occur very often and the levels are considered to be acceptable.

5 Identification of law enforcement needs

The statistical analysis below indicates the factors that can enable the future effectiveness of cross-border information exchanges. The major enablers are legislative conditions, trust, technical conditions and co-ordination issues. Although they were not directly evaluated in the questionnaires, in the interviews “staff operators” skill and experience were also stressed. This latter is a sensitive one, but it is crucial.

Table 9: Perceived factors enabling information exchange between EU MS and with EFTA countries - Police and Customs Authorities (read left to right: major obstacle to no obstacle)





5.1 Access to data

Throughout this section, “direct access” means that an officer of a MS can themselves obtain access to the databases of another MS. It does not refer to the ability to gain access almost immediately by asking a colleague from another MS to provide this data (e.g. if they are collocated in a P(C)CC). The latter case is deemed to be “indirect access” even if it is sometimes referred to by MS as direct access.

In most cases MS do not have direct access to other MS databases or to third country databases on bilateral or multilateral bases, except for the Prüm DNA and fingerprint exchanges. The majority of MS are of the opinion that there is no immediate or intermediate need for such access, while a few MS would prefer having at least a limited access to some databases in other MS in line with the Principle of Availability. Some MS stated that they would like direct access for limited purposes in relation to specific crimes closely linked with cross-border movements, such as sexual offences against children.

Some MS indicated that it would be very useful to have direct access to foreign databases on suspects’ criminal activities (criminal intelligence registers), on criminal records (a record of a person’s criminal history) and on genuine ID databases in order to verify identities. It should be stressed that sometimes requests related to the above mentioned categories may take months. A pilot project between The Netherlands, Belgium and one German federal state, which is still under consideration, seems to be a possible forerunner for wider introduction and the extent of access for German policemen would be likely to be the same as it is for Netherlands policemen. In relation to the LEA’s business needs, a possible further development of direct access to other

MS's databases seems to be more beneficial for introduction between neighbouring countries (in the first stage) before an EU wide solution is sought.

Member States have indicated the following possible obstacles which might thwart access to other MS's databases:

- data protection issues
- incompatibility of records
- language problems
- different legal systems
- uncertainty if a user in one MS would get the correct information if s/he is not familiar with the foreign system (language, logic, etc)
- uncertainty if information in other MS is up-to date and valid, etc.
- uncertainty if MS are willing to open their own databases to other MS
- 27 or even more databases are not interoperable and data extracted from one cannot easily be entered into another

The majority of MS are very keen on further development of HIT/NO-HIT systems for cross-checks in different MS databases, rather than having direct access to other MS databases. This could simplify inquiries because not each and every MS would need to be asked, and currently many requests result in negative responses because no record exists in that MS. An early automatic HIT/NO-HIT system would therefore eliminate the need for superfluous detailed information requests. The HIT/NO-HIT system is an excellent concept requiring a proper back-office system, which in turn requires additional resources arising from the need to provide further details on what is "beyond" the HIT. HIT and NO-HIT responses should be extended to providing, automatically, basic details such as file number and responsible authority in another MS, where possible (this will require common definitions). Examples include mobile phone or land line registration, or bank account existence – not content – details which would further verify whether a given identity is correct. These points were especially stressed by France and Italy.

Although there is an idea to develop a European Police Records Index System (EPRIS), this could be done similarly to the European Criminal Records System (ECRIS). Concerning ECRIS, exchanges of information on convictions among a few EU MS work quite well, whereas among others it works only on request. In some EU MS police authorities have a direct access to those kinds of data (e.g. The United Kingdom) while in the other MS this is not a case, with these categories of data in the domain of the Ministries of Justice. Several MS, especially the UK, expressed concerns about how well ECRIS will work, especially in relation to "collateral" increased workloads, as the faster and more complete exchanges of criminal conviction records leads to further requests for information and intelligence about or from the convicted person. It was urged that the pilot operations of ECRIS be subject to detailed operational evaluations.

According to interviewed MS, HIT/NO-HIT systems could be established for the following categories of data:

- existence of criminal intelligence for a person
- criminal records (convicted persons)

- denounced suspects (not convicted but reliably identified)
- hooligans and violent demonstrators
- ballistics (firearms) information
- citizens register (for identification purposes)
- register of sex offenders
- telephone subscriber details and telephone registration data (in this case it would no longer be necessary to send requests only to get the response that it is a pre-paid SIM card number and formal requests would only be sent if the number is registered to a person or entity).

Concerning telephone subscriber details and telephone registration, it is open to question as to whether this could be implemented in the future because data on telephone users is usually not kept by the LEA but rather by the telecommunication companies, and it is hardly possible to integrate databases into the HIT/ NO-HIT bases. Also in many states a court order is necessary to acquire such information. However, the Project has noted the degree of emphasis made by MS regarding the importance of obtaining such access, not least as it may increase the likelihood of the identification of persons.

MS are divided on the topic of centralisation of cross-border information exchange: some MS do not see a need that more of their national staff should have direct access to foreign information sources such as databases or contacts for co-ordination and control reasons. According to these MS, this would lead to a loss of awareness at central co-ordination level, of who is contacting whom, for what and when. Exchange of information, according to these MS, should be done through central levels which need to have an overview of the incoming and outgoing requests; otherwise it would be difficult to supervise the exchange of information.

Following on from the issue of direct access to foreign information databases, the issue of direct communication between LEA's should be mentioned. Although some MS are reluctant to enable direct communication between national regional staff or investigators and regional staff and investigators in other countries, this should be reconsidered in the future. According to some MS, this could contribute to more efficient and expeditious information exchange and the central authorities' fear of losing control could be overcome by an automatic copying system to national authorities about the communication made between regional authorities. For this reason, throughout this Report, the issue of setting up "all agency" national central administrative registers of cross-border exchanges has been stressed.

The aspect of centralisation of data is also important on the European scale: the Information System (IS) at EUROPOL is one of the EUROPOL's two main systems for the storage and analysis of personal data. The purpose of the IS is to support Member States and EUROPOL, as well as EUROPOL's partners. All MS have direct access to the system in their EUROPOL National Units and via their EUROPOL Liaison Officers, in order to make enquires in the system and to insert data. Third States and organizations which have operational agreements (e.g. Australia, USA, Canada, etc) may also have indirect access, through EUROPOL, to the information in the IS, and they may also contribute to the system by sending data to EUROPOL. The IS does not just store data and make it possible to search and retrieve it but also provides a visualization tool and supports the automatic detection of possible hits between different investigations (cross-border crime check functionality – CBCC). The CCBC functionality can automatically detect communication links between telephone numbers in different criminal cases. The IS can, however, only be as good as the input; without input there is no Cross-border Crime Checks and LEA's shall consider uploading data from their cases more pro-actively to the IS.

According to MS, access to "non police data" such as EURODAC, EU-PNR should be accessible to the police authorities in the future. The EURODAC database should be used for the identification of criminals who are found amongst illegal immigrants. Such access is seen as strongly assisting the police to fight against crime more efficiently, but this should be limited to the most serious offences and to those in imminent danger. One option would be to start with those offences covered by the European Arrest Warrant (32 types of offences).

5.2 Time Limits

Although overall requests have risen across the EU, an increase of urgent requests has not been noticed. MS indicated that responses from abroad are mainly received within generally agreed and reasonable time frames. However, there are felt to be particular MS which are often late in replying. Problems occasionally occur with the exchange of supplementary information in relation to article 96 SIS (refusals of entry to third country citizens) where MS do not respond instantly, which sometimes causes delays and inconvenience when a person concerned is being held at a border crossing point.

The existing classifications regarding urgency seem to meet LEA's needs. However, some MS are of the opinion that unification of definitions between MS and agencies such as EUROPOL, INTERPOL etc. would be useful. Moreover, a unification and simplification of the existing classifications would be good (e.g. only 'urgent' and 'non urgent', while 'very urgent' is superfluous as 'urgent' already means that a quick response is of high importance) and perhaps a category of 'immediately' should be added when an immediate reaction is required from another MS (e.g. for checks being made at the external border). The deadline of 8 hours set according to the SI is too long in such cases. However, the key point is that the reasons for the urgency are explained, another example of the importance of giving explicit reasons for requests.

According to MS, there is no common understanding of the term "urgent" and "not urgent" and some countries use "urgent" or "very urgent" in almost all cases. Clearly, with INTERPOL exchanges, there are too many "flash/urgent" notifications. MS may consider their own cases or requests urgent or very urgent although the receiving MS cannot understand the urgency. For instance, a MS' national legal requirements, where a case has to be submitted to the court within 3 days, may require a very quick answer, although the case itself does not seem to be either important or urgent. Almost all MS are of the opinion that clarification over why a case is urgent should be given and really urgent cases would be dealt with immediately (e.g. by phone, fax, etc).

Sometimes LEA's are late in providing information to a LEA in another MS. According to MS, the main reasons for delays are the following:

- internal processes when requests are internally sent to other state institutions within the country

- unavailability of information
- lack of personnel to deal with the request
- need to obtain legal approval for exchange
- technical problems in retrieving data (system failure etc)
- prior court permission being required or information having to be obtained from other domestic institutions
- complexity, scope and nature of the case or cases.

The time required for preparation of a response varies between authorities who are being tasked to prepare answers and sometimes it takes longer when local or regional units are responsible for preparation of the answers. Nevertheless, some MS inform the requesting partner in case a delay is foreseen with an interim response, which seems to be a good practice and should be made into a standard.

5.3 Quality of information and criminal intelligence

The quality of information or criminal intelligence received through the international channels is generally good. Although there are no specific criteria for assessing the quality in EU MS, the first important quality indicator is the speed of response, and secondly, that all questions are answered. The information also needs to be accurate, helpful for LEA's, and complete. If a response does not fulfil all these aspects, it is not a quality answer. The quality of the answer also depends on the country, culture, the quality and duties of the personnel receiving and preparing information (e.g. language problems, time of the day received, which can affect which person or unit receives the information), and level of awareness of the legal framework, and of course on the quality (e.g. clarity and completeness) of the request itself. INTERPOL and EUROPOL have established quality assessment processes for the evaluation of the quality of information which endeavour to raise the quality of information and intelligence provided by MS. These should be actively considered by MS for general adoption on an all agencies basis within MS, and in concert with neighbouring MS and then on an EU wide basis.

According to some MS, the quality of responses would be higher in cases where the requesting MS states would reveal their background information (i.e. reason for request). Not surprisingly, the level of the quality is usually higher between MS that use the same language.

The quality of information exchanged through different communication channels is not directly comparable because communication channels have been established for different purposes. When the SIS communication channel is being used, prescribed forms are used and it is also possible to add a free text. However, when communicating with INTERPOL and EUROPOL, there is a greater reliance on free text and this may sometimes cause problems in understanding the messages.

The prescribed classifications related to the reliability of information (e.g. Swedish Initiative, EUROPOL 4/4 classification, etc.) are properly used. It sometimes happens that information is wrong or misleading but this is because of misunderstandings and is not intentional, and only in a very few cases is information felt to be deliberately wrong or misleading.

Clarification requests are generally not needed very often. Follow up questions are more common because new information leads to new questions and some countries ask why the authorities need this information or criminal intelligence in follow-up correspondence. In addition, the numbers of clarifications and follow up question vary from country to country and depend on the circumstances of the case (e.g. complexity) and to some extent on the quality of the request. Sometimes clarification is even needed internally for domestic requests before they are sent to other MS. Generally speaking, follow-up questions or clarifications are not seen in a negative sense but as positive developments.

The quality of staff employed in units responsible for international exchange of information has a direct impact on the quality of information provided. The importance of language skills, operational experience and good knowledge on related legal issues were specifically stressed by MS.

6 Good practices

Many good practices were identified in visited MS. The term “best practices” was intentionally not used, as identified good practices were not commonly agreed upon and they may not be applicable in all MS, depending on national systems and regulations.

- Use of Single Points of Contact (SPOC) for international communication (e.g. Austria, Estonia, Denmark). While this is recommended in the Schengen Catalogue it is not implemented in all MS[44].
- Mutual exchange of SPOC staff and other personnel in order to acquaint staff with the structure and proceedings of cross-border exchange of information with other MS, e.g. between “internal” MS and those with external borders, to Spanish / French SPOCs in relation to counter terrorism work, and between MS whose exchanges are largely carried out by one agency – usually the police – and those where several agencies – regional police, national serious crime agency and customs - are involved in cross-border exchanges (e.g. Slovenia with Estonia and other Baltic States, all four states being external border states)
- Exchanges of personnel internally between NCB, ENU and SIRENE (e.g. Denmark) also contribute to familiarisation with other national central units for cross-border exchanges and their procedures.
- Regular briefings to regional and local units by NCB and ENU staff to increase the knowledge of the role and capabilities of INTERPOL and EUROPOL and to motivate them to share information with these organizations, as is the French practice.
- (National) Handbooks for International Exchange of Information, such as are compiled in a few MS like Slovenia and Finland; they significantly contribute to the clarity of procedures and more effective exchange of information and intelligence.
- Clearly outlining the purpose of the request in all information exchange requests, as this ensures the relevant agency or agencies are contacted, and that the proper procedures are applied; this point was stressed by all MS visited.
- Where a request has been sent to the “wrong” agency, forwarding it on to the correct one, while immediately informing the requesting agency as to where jurisdiction lies; again, several MS, including Slovenia and Finland, pointed this out as their practice.
- Automatic definition of internal deadlines for incoming requests and automatic monitoring of the timely settlement of the answers: automatic reminders or a case management system that notifies when a response is not prepared within the deadline. This has been introduced in Slovenia, Austria and some other EU MS. In Slovenia, for example, the deadlines are also set for outgoing requests in order to enable case officers to send a reminder if there is no response from abroad on time.
- When authorities cannot reply within the deadline or only partly, they inform the concerned MS within the deadline about the reasons and provide an interim response with information gathered by that time (e.g. France).

[44] Schengen Catalogue, Recommendations and Best Practices, volume 4, Police Co-operation

Ø Placing of liaison officers at the host country's central authority's offices responsible for cross-border international exchanges, as opposed to placement in Embassies (e.g. as is already done in Estonia and Italy). This significantly facilitates immediate contacts between liaison officers and the central authorities.

Ø The use of strong and highly co-ordinated multinational Liaison Officer Networks as in the Nordic countries (e.g. Finland, Denmark), with a LO of one MS being responsible for assistance to other MS.

Ø Use of SIENA significantly facilitates direct communication between MS. This was stressed e.g. by the Netherlands, and may reduce the number of liaison officers within the EU, enabling redeployment of resources to non-EU countries.

Ø Joint Investigation Teams (JITs), including Customs personnel, facilitate and improve cross-border information exchange, including the prioritization of case work and requests; e.g. cigarette smuggling JITs as currently carried out by Austria with Germany and soon with Hungary, Slovakia and the Czech Republic, and with the co-operation of, or observation by, EUROPOL and OLAF

Ø Successful activity of P(C)CCs and SCCOPOL in France could serve as an example of inter-institutional joining of functions of customs and police authorities

Ø Participation of agencies to which cases are referred for contribution (e.g. Prosecutors, Justice Ministries, EUROJUST) through combined training on completeness and quality issues and on exchange procedures (based on the reported examples of the Austro-Spanish-Greek investigation of a large group of alleged Georgian Mafia suspects in March 2010, or sensitive and resource intensive surveillance operations against cross-border paedophile suspects mentioned by Italy and the subject of UK-Spanish information exchanges in the summer of 2010)

Ø The new (mid 2010) updates to the OLAF administered EU AFIS databases for Customs matters, which allow simultaneous updates of multiple databases from one input of data, could serve as models for "central register" databases within MS and across the EU, such central registers providing widespread viewing rights without compromising MS control over ownership of sensitive or operationally significant details.

Ø Proactive delivery of intelligence (in its widest sense, including actual and potential trend information) which may not be of obvious or immediate interest or benefit to the agency or MS concerned; Germany, the Netherlands, Belgium and the United Kingdom are especially proactive in providing data to EUROPOL and INTERPOL.

7 Recommendations and conclusions

7.1 Conclusions

The level of cross-border information exchange has significantly increased in almost all EU MS over the past few years. At the same time, the numerous legal acts and communication channels currently in place have led to a wide choice and created an extensive toolbox for collecting, processing and sharing information between national authorities and other European players in the area of justice, freedom and security. This variety, however, sometimes leads to confusion by making available several appropriate channels, and – given the lack of a common European policy - law enforcement agencies and MS sometimes differ in their choice of preferred communication channels.

Generally, while there is room for improvement in terms of standardisation and rendering information flows more efficient, cross-border exchange of information between EU MS and with EFTA countries can be said to function reasonably well. MS LEA largely trust each other and requests are generally answered in an acceptable timeframe, including those considered urgent by the senders. The related classifications largely meet LEA needs. Also the quality of information and intelligence received in terms of completeness and accuracy generally seems to be good. MS did not identify major redundancies and bottlenecks in the procedures for international exchange of information.

Based on in-depth assessment of the situation in the Focus Countries visited, together with evaluations of the answers to the questionnaires supplied by the other Member States, it is the conclusion of the Project that the views of the MS are generally not significantly different in relation to operational collection and exchange of evaluated information, despite very different legal, historical, geographical and structural backgrounds resulting in very different respective competencies of authorities and national structures. These national structures naturally have a large impact on work flows, also related to international exchange of information; SPOCs are in place in many countries and seem to be one of the most efficient tools for efficient cross-border exchange of information. The quality of personnel is key in this regard, as staff has to know their own national structures and systems, as well as those of other countries, and be able to formulate requests and their background well.

The Principle of Availability, as a vision of eliminating national borders in terms of information exchange, works only partly in practice. It is almost impossible to reach its full potential as there still exist different national systems, data bases/registries, legal systems, data protection legislation, and also significant interoperability problems. Legal obstacles, which do exist and hamper efficient cross-border information exchanges, mainly relate to differences in national legislation rather than to the EU legislation. At the same time, different interpretations of EU legislation also sometimes lead to legal and practical problems.

It can be established that the Swedish Initiative has not facilitated the exchange of information or criminal intelligence among MS as initially envisaged, with only a few Member States using the Swedish Initiative and its form. In contrast, the Prüm Decision seems to be one of the most efficient tools to identify criminals and solve crimes, although its purpose is not to exchange information or criminal intelligence as such, but enables EU MS almost instantaneously to know if a certain type of information is available in another MS or not. No MS experienced serious problems in implementing the Decision. Problems generally arise only at the stage of follow-up requests, specifically where Letters Rogatory are required. Research done among EU MS indicates that further development should rather go towards the development of new HIT/NO-HIT systems than to opening national databases to other MS law enforcement authorities. MS are weary about the introduction of new systems, also in light of problems with coherence of data, and the focus should clearly be on efficient and effective implementation of systems and procedures currently in place.

In the course of the study it became evident that there is a lack of statistics on international exchange of data, specifically also regarding the types of information and categories of data exchanged. Comparability naturally is a specific challenge in this regard. Despite this, it can be said that data about persons and vehicles, financial data and communication data are very often exchanged on a European level, and a significant need to simplify exchange specifically of telecom data was expressed.

In terms of technical capacities, probably more in the area of customs than in the police area, there are significant differences regarding the physical and electronic (encryption) security of information exchange networks which are reflected in limitations on what some MS can send to other states. This also contributes to the considerable use of outdated methods of communication, often involving postal mail.

While an increasing level of mutual exchange/access of data between agencies on a national level has been noted, work flows for customs and police authorities do still seem to run in parallel and even closer cooperation is needed. On a European level there are positive signs in this respect, with the planned direct secure access by EUROPOL and EUROJUST to the AFIS systems operated by OLAF from May 2011. Worrying especially regarding the databases on EU/international level is the apparent lack of pro-active provision of information by MS. This poses a problem as, naturally, databases are only as good as their input.

Although the role of EUROPOL is becoming more and more important, it should not be forgotten that Europe is only one region of the world and the worldwide police and law enforcement co-operation and exchange of information should not be overlooked. The fact is that some MS have recognized the capabilities of institutions such as EUROPOL, INTERPOL, EUROJUST, OLAF, etc. and they provide and share information and intelligence with them to a significant degree. Many MS made it clear that they see increased co-operation with EUROPOL as vital in the future.

When it is intended to use acquired information as evidence, in certain cases it is expedient to include EUROJUST into the process of information exchange or to consult prosecutors of different MS residing at EUROJUST in respect of admissibility of evidence and other legal issues.

To conclude, despite ongoing improvements and existing plans for the future, there is still room for significant improvement, especially with providing and sharing information among EU MS law enforcement authorities and the multilateral institutions such as EUROPOL and INTERPOL Currently, a few MS are sources of data input to EUROPOL's and INTERPOL's databases. Although EUROPOL and INTERPOL have been established to provide services to MS, law enforcement authorities do not yet use their capacities sufficiently. MS should more actively contribute to the further development of those institutions in the future, more clearly express their needs and more often ask for their assistance in EU MS operations. The further development of mutually associated projects between EUROPOL, INTERPOL, EUROJUST, FRONTEX and OLAF and the MS presents the greatest challenge for the future, but also the greatest opportunity.

Table 10: Key Findings related to the hypotheses for this study

Assumptions	Key findings
Obstacles to free circulation of information currently exist	Free circulation of information and criminal intelligence is impeded to some extent due to the existence of different obstacles, such as differing legal interpretations of what can be delivered, lack of secure electronic exchange networks in certain cases, and differing agency jurisdictions within and between MS.
There is no clear policy on information channels	MS have their own approaches on the selection of information channels. Policy on the selection of information channels varies from country to country. This does quite often lead to internal MS co-ordination challenges, and in some cases duplication of cross-border information exchanges.
Information is divided into different groupings which do not interact	In some countries information requests are divided into different groupings or departments which do not interact among themselves properly. As stated immediately above, this does lead to considerable duplication of effort. Effective exchanges between MS are heavily dependent on effective co-ordination within MS between agencies and between national, regional and local units, particularly in larger MS.
Legal barriers hinder exchange of information	Legal barriers often hinder exchange of information and criminal intelligence. Examples include significantly different requirements before information supplied is usable as court evidence, disclosability of information (especially telecommunication and financial data) and different interpretations of the appropriateness of a legal agreement in relation to compelling witnesses to give information.
Technical barriers hinder exchange of information	Technical barriers do occasionally hinder exchange of information and criminal intelligence, and primarily hamper a greater interoperability among different IT systems. Such barriers in some places include lack of secure email systems resulting in inability to send high security material, and widely differing software capabilities resulting in information transfer capacity limitations and delays due to the need to reformat attachments.
Practical barriers hinder exchange of information	Practical barriers do occasionally hinder exchange of information and criminal intelligence. In addition to legal and IT /communications barriers, practical barriers include availability of SPOC staff and sufficient and properly trained staff to research requests, retrieve all relevant information and produce quality replies. Staff training and capabilities are crucial.
Law enforcement authorities do not fully trust each other	Law enforcement authorities generally do trust each other. There were no indications that information was withheld due to concerns about integrity and/or leakage of information.
Member States are reluctant to transfer information to EUROPOL	Some MS are reluctant to transfer information to EUROPOL or to provide information and criminal intelligence to EUROPOL more

	proactively. Awareness of EUROPOL's capacities should be raised, as was highlighted by the desire of most MS to increase co-operation and to introduce and share common good practices.
EUROPOL does not fully meet the demands of law enforcement authorities	EUROPOL does largely meet the demands of law enforcement authorities. Many MS expressed strong desires to increase co-operation. There was however some confusion regarding the demarcation of EUROPOL's remit.
Effective and expeditious exchange of information and intelligence is seriously hampered by time consuming procedures, over bureaucratic administrative structures and legal obstacles and differences in Member States' legislation	Effective and expeditious exchange is indeed hampered due to these factors. Widespread and deep awareness of each other's systems and procedural requirements needs to be significantly increased.

7.2 Recommendations

The recommendations derived from the conclusions as well as those brought forward by MS representatives during the interviews can be roughly divided into the areas of handling of requests, standardisation, data access, human resources (in awareness and exchanges of personnel, as well as training), liaison officers, and co-operation with organisations on EU level.

Handling of requests

- Single Points of Contact (SPOCs) for all channels, including police and customs channels - 24/7, adequately resourced and suitably staffed with permanent staff. This ensures integrity of received and sent information and enables agencies within and across MS to avoid unnecessary duplication of information; the use of permanent staff encourages personal relationships between SPOC personnel of different MS.
- Mutual access for SPOC staff to Police, Customs and other currently separated databases within MS in order to ensure that SPOCs are fully informed for the purposes of exchanging information internationally.
- Central registration by SPOCs ("administrative registers" or "logbooks") of all exchanges on international level, including basic details of the requests, and data necessary in cases of illegal use of personal information; this is vital especially in large MS with multiple agencies and/or significant exchanges being made by Regional Agencies.
- Integration of exchanges between Financial Intelligence Units (FIUs) with basic registers and mainstream databases to maximise the integration of financial data with persons of interest
- Attention to be paid to maintaining the continuous flow of information from the bottom to the top (and vice versa) on an intra-service level in cases of institutional changes, e.g. where border police agencies are integrated into the police.

- In order to assist SPOCs, information requests should be made as modular as possible with reductions in free text use, with the legal authority and purpose of the requests being clearly stated – the Siena format is a particularly suitable model
- When authorities cannot or only partly reply within the deadline, they should inform the concerned MS within the deadline about the reasons and provide an interim response.
- Forwarding misplaced requests to the correct authority, immediately informing the requesting party thereof.
- When a request is denied, it is recommended to state the reasons why an authority cannot comply and, crucially, suggest alternative ways of how to obtain equivalent information.
- Active consideration by MS of adoption of INTERPOL/EUROPOL quality assessment processes on an all agencies basis for the evaluation of the quality of information

Standardisation

- One common language (preferably English) should be used for all - but especially urgent - requests as in MS employees with a sound knowledge of English are generally available all of the time.
- Clearly understood definitions of often confused terms regarding information databases, the legal procedures and channels for exchange of data from these databases, and the technical (especially IT) means used to transmit data; these points were specifically stressed by EUROPOL and OLAF.
- Harmonization and detailed clarification of the classification of data types (e.g. what types of data should be classified and to what level); an indicative system, issued with recommendations explaining the identical, similar and different definitions within MS
- Formal agreement on the handling of matters which are priorities in the requesting state but not in the receiving state; consideration has to be given to meeting the requesting states needs within agreed criteria
- Use of existing priorities (e.g. urgent) as agreed
- Recall existing agreements on the default method of exchanging information for the different channels and take necessary steps for their implementation (ideally secure email to secure contact points)
- Availability and comparability of statistics need to be improved (see chapter 3.3. and 3.4). The Project has made suggestions about how information requests, replies and proactive offers of intelligence might be categorised, in order to enhance procedures for the easy availability of relevant data for the purposes of evaluating comparative resource demands on MS.
- Ideally, an EU-wide common basic Handbook for Information Exchange should be compiled, addressing the above issues and laying down qualitative best practice procedures (e.g. whether an agency receiving a request proper from another agency forwards it on, or returns it to the requesting authority). This should be issued in such terms that it does not preclude MS using their own procedures for reasons of national legislation or policy. Such handbook should be based on existing guidelines and manuals, and judicial authorities should be involved in drafting.

Data access

- Increased access to HIT/NO-HIT data such as is being exchanged under Prüm: the purpose is to avoid unnecessary further checks on persons who are not of interest, and to more fully identify persons who are.
- This could first be introduced between neighbouring MS, as most information exchanges are between neighbouring MS; starting with basic police information (HIT/NO-HIT, yes/no data) with safeguards of citizens rights built into the procedures; the results of the Pilot Project, which is being developed by The Netherlands, should be considered in the future.
- There is a general consensus that a common EU wide investigation and intelligence database is very much a long term aim; more immediate steps suggested include the need for significant reductions in the number of "partial" databases and a move to common all agency databases within MS, with appropriate safeguards
- The use of INTERPOL's Stolen and Lost Travel Database before issuing visas at the EU MS consulates should be examined. A feasibility study is being carried out by Germany in this regard.

Increased Awareness and Exchanges of Personnel

- Emphasis should be placed on greater awareness of each other's SPOCs and their common and differing organisations, competencies and capabilities.
- This could be achieved by access of all MS Agencies to a directory outlining the details of SPOCs across the EU
- Access to sample MS National Handbooks on Police Co-operation and Exchange of Information – possibly through a restricted EU wide Intranet
- The Naples II Handbook relating to exchanges on Customs information and investigations warrants widespread distribution to police agencies and judicial authorities, especially in MS where investigations of customs offences are carried by the police or directly under the supervision of the judicial authorities
- Enhanced mutual exchange of SPOC staff or other staff involved in international exchange of information, as a highly effective way to share working practices and to increase the operational awareness of legal instruments, operational procedures, information network technical systems and capabilities, of both the capabilities of databases and their operational uses, of MS priorities and organizational structures. The use of central EC funds to finance such exchange should be considered so that those MS subject to severe budgetary restrictions are not disadvantaged
- Similar consideration should be given to exchanges between P(C)CCs staff, and between P(C)CC and SPOC personnel: an Internet or video link based P(C)CC information Awareness Network should be considered, with central funding being made available to assist MS whose budgets are limited: the purpose would be to exchange good practices in live, face to face, operational circumstances
- Increased exchanges of staff for special occasions (police operations, police raids, police checks, mirror investigations, sports events, etc) and the deployment of police

officers or criminal investigators for investigation purposes with the investigation agencies in other MS.

- Awareness of the fact that, unlike often mentioned, there is no major lack of trust between Member States' LEAs should be increased

Training

- Enhanced participation of agencies to which cases are referred for contribution (e.g. Prosecutors, Justice Ministries) in training on completeness, quality and exchange procedures to increase awareness of international police co-operation tools: some judicial authorities are not very eager to expand their investigation beyond national borders although this would be possible and beneficial.
- Possible development of the common curriculum (CEPOL) for the personnel engaged in cross-border exchanges
- Common training with neighbouring countries
- Increased language courses

Liaison Officers

- Consideration should be given to making wider use of Liaison Officer Networks, as in Nordic countries, as a model for other neighbour to neighbour, regional and wider LO networks, with a LO of one MS being responsible for assistance to other MS

Co-operation on EU level

- Awareness raising amongst MS of existing systems developed by different organizations: e.g. INTERPOL, and EUROPOL's role in intelligence gathering and analytical capabilities
- Wider use of the possibilities for EUROJUST to organise and co-ordinate meetings between prosecutors and representatives of other LEAs
- Enhanced co-operation between international organizations such as EUROPOL and INTERPOL and EU MS. On the one hand EUROPOL should be more often included in EU MS criminal investigations - there are a lot of analysts available at EUROPOL in order to support MS - while on the other hand EU MS should more proactively provide information and criminal intelligence to EUROPOL and INTERPOL.
- Greater use of EUROPOL as a primary communication channel and information source as a key factor in boosting efficiency, especially as MS increasingly have both police and Customs personnel based there and the AWF data is increasingly used. The network of Liaison Officers stationed at EUROPOL in general permit a quick exchange of information on a trustful basis.
- Creation of a 24/7 ENU operational desk(s) in all EU MS, which is necessary for the information flow within the EU Member States.
- Culturally, there need to be significantly greater efforts made to encourage proactive delivery of intelligence (in its widest sense, including actual and potential trend information) which may not be of obvious or immediate interest or benefit to the agency or MS concerned, but would be to another MS; some forms of internal and quantitative, but especially qualitative performance measures should be considered to provide incentive for such delivery. This is particularly important for ensuring new technical

upgrades such as the introduction of the MAB system (secure communications system for simultaneous update of multiple databases) by EU OLAF to be fully utilized, especially given that these systems will be directly accessible by EUROPOL and EUROJUST from May 2011. The increased possibilities arising from much greater and easier data sharing between EUROPOL and OLAF will also enable the early setting up (in 2011 and 2012) of co-ordinated "results recording procedures" for the measurement of how proactive information is being delivered and how this improved co-ordination is translating into operational results, and assist in closer coordination of intelligence and investigation of Customs matters, both in relation to violations of national legislation and also offences against the Community budget.

- Particularly, NCB and ENU should increase the awareness amongst their colleagues of the role and capabilities of INTERPOL and EUROPOL, especially at local and regional levels, and encourage them to share the information more widely and spontaneously with these organizations.
- Merging of the advantages of particular communication channels should be more often used. For example, enhanced co-operation between EUROPOL and INTERPOL, where EUROPOL may provide the analytical support, and INTERPOL makes use of its global reach, could serve as a very good example (e.g. dealing with Maritime Piracy is one very good example concerning efficient co-operation between EUROPOL and INTERPOL).
- Co-operation between EUROPOL and OLAF should be strengthened, with the specific involvement of EUROPOL's significant quantitative and qualitative analytical capability, and its AWF – Analytical Work Files - capability. OLAF's oversight of the AFIS systems, including CIS as an EU wide intelligence database for Customs matters, and its analytical capabilities, mirrors EUROPOL's EU wide capabilities, so that co-operation is likely to be highly effective in relation to resources deployed.
- More and wider involvement of Joint Investigation Teams (JITs) at the EU level, including Customs personnel, would facilitate and improve cross-border information exchange.
- No major new information exchange communication systems and intelligence databases – be it on national or international level - should be introduced without first examining existing, in progress or planned equivalent databases in MS, and with the resulting decisions being notified in technical and operational terms to other MS and to EUROPOL and where appropriate to FRONTEX, OLAF and INTERPOL; in particular the intention to introduce major new databases should be notified to all other MS and to EUROPOL and other relevant EU or European wide agencies with brief explanations of their functions and operational impacts. According to some EU MS, the newly established Standing Committee on Operational Co-operation on Internal Security (COSI)[45], which is a body of the Council mandated to facilitate, promote and strengthen co-ordination of operational actions between EU Member States in the field of internal security, should take part and take over an important role in this field. In the establishment of new solutions on EU level, close cooperation between all relevant European Commission DGs, such as DG HOME and DG TAXUD, is also essential.

[45] COSI was established on the basis of the Treaty of Lisbon (Art. 71 TFEU) with the Council Decision on setting up the Standing Committee on operational co-operation on internal security, 25 February 2010

8 Bibliography

- Commission Decision of 4 March 2008 adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II);
- Communication from the Commission to the European Parliament and the Council; Overview of information management in the area of freedom, security and justice, Brussels, 20.7.2010 COM(2010)385 final
- 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, Official Journal L 239 , 22/09/2000 P. 0019 – 0062
- Convention on Mutual Legal Assistance in Criminal Matters (2000 MLA Convention), 29 May 2000
- Council Conclusion on an Information Management Strategy for EU internal security, "2979 JHA Council meeting, Brussels, 30 November 2009 (doc. 16637/09 JAI 874 CATS 131 SIM 137 justciv 249 JURINFO 145)
- Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p.1
- Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information; Official Journal L 332 , 17/12/2009 P. 0017 – 0022
- Council Decision on setting up the Standing Committee on operational cooperation on internal security, 25 February 2010
- Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the MS of the EU
- 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 - Guidelines
- Council Joint Action 98/700/JHA of 3 December 1998
- Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism
- Eurojust Annual Report 2009, http://www.eurojust.europa.eu/press_annual_report_2009.htm
- EUROPOL Strategy 2010-2014, http://register.consilium.europa.eu/pdf/en/10/st06/st06517.en10.pdf
- External evaluation of the European Agency for the Management of Operational Cooperation at the External Borders of the member States of the European Union, Final report January 2009. COWI A/S
- Guidelines on the implementation of Council Framework Decision 2006/960/JHAof 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union
- Manual of Good Practices concerning the International Police Cooperation Units at National Level (7968/08)

Ø Opinion of the EDPS on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)

Ø Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

Ø Regulation (EC) No 863/2007 of the European Parliament and of the Council of 11 July 2007 establishing a mechanism for the creation of Rapid Border Intervention Teams and amending Council Regulation (EC) No 2007/2004 as regards that mechanism and regulating the tasks and powers of guest officers

Ø Schengen Catalogue, Recommendations and Best Practices, volume 4, Police Cooperation

Ø Schengen Investigated, A comparative Interpretation of the Schengen Provision on International Police Cooperation in the light of the European Convention on Human Rights; Chantal Joubert & Hans Bevers; page 11

Ø Swedish Initiative (Council Framework Decision2006/960/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)