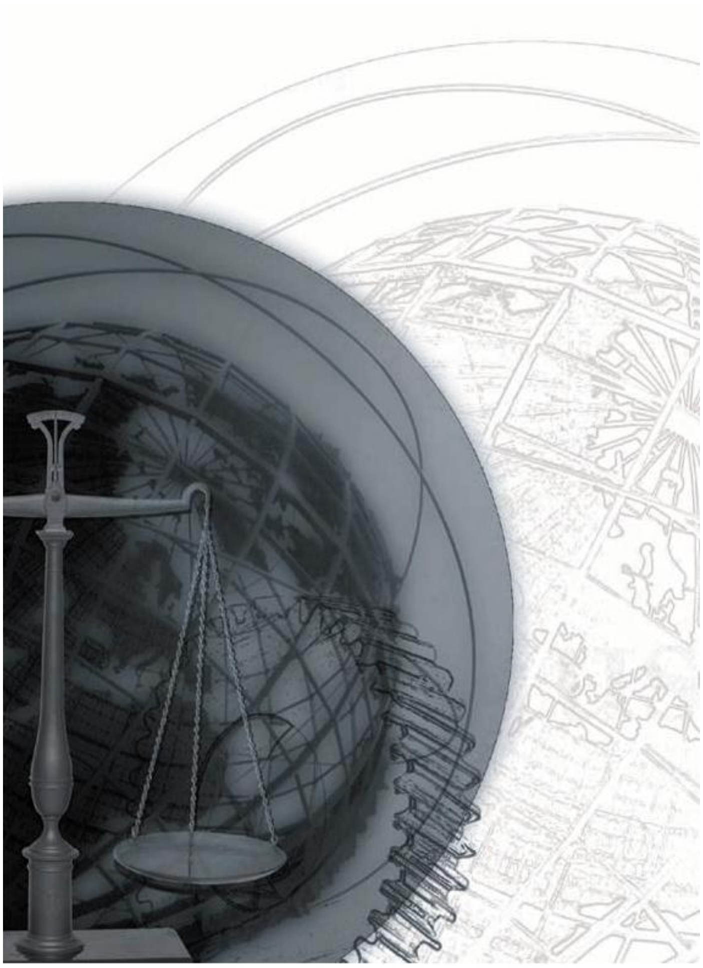


DG Home

Study on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records Index System

EPRIS

Final Report

Version 2.00

08.10.2012

European Commission

Produced by

Unisys

IRCP

Disclaimer

This report has been prepared for the European Commission by Unisys Corporation and the Institute for International Research on Criminal Policy (IRCP) of Ghent University. It reflects views only of the authors and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Authors:

Jeanine Focant
Giedre Kazlauskaite
Wilfried De Wever
Marc Lombaerts
Tim Meulemans

Prof. Dr. Gert Vermeulen
Vincent Eechaudt
Dr. Wendy De Bondt

Table of Revisions

Ver.	Date	Author	Description	Action*	Page
0.01	30/04/12	VE	Section 5.3	I	42-43
0.02	15/05/12	GK	Sections 2, 4, 5.2, 5.5.3, 6	I,R	7-10; 29-34; 36-41; 54-55; 59-106
0.03	23/05/12	WDW	Sections 3, 5.1, 5.4, 5.5	I	11-28; 35-36; 44-53
0.04	06/06/12	ML	Section 5.5.4	I	56-58
0.05	08/06/12	TM	Section 5.2. and 5.5	I	36-38; 44-53
0.06	10/06/12	GK	Consolidation of all sections	I,R	All
0.07	12/06/12	WDW	Section 1	I	5-6
0.08	13/06/12	GK	Integration of comments	I	All
0.09	14/06/12	JF	Review	I	1-58
0.10	15/06/12	WDW	Final review	I	All
1.00	15/06/12	GK	Delivery of draft version	I,R	All
1.01	10/08/12	GK	Integration of comments	I,R	All
1.02	21/09/12	GK	Final version	I,R	All
2.00	08/10/12	GK	Final delivery	I, R	All

(*) Action: I = Insert R = Replace

Table of Contents

Table of Figures

Table of Tables

1 Executive Summary

This report reflects the outcome of the study on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records Index System (EPRIS). Its main objective was to investigate the need and possible approaches, in particular the establishment of a European Police Records Index System (EPRIS), for identifying whether police records related information is available in one or several EU Member States.

A common understanding of terminology and purpose is crucial in any case. Based on an enquiry related to available police record definitions in the Member States, the study team suggests the following definition to ensure a common terminology of a "police record" at EU level: A 'Police Record' shall mean any information available in the national register or registers recording data of competent authorities, for the prevention, detection, investigation and prosecution of criminal offences.

To obtain a better understanding of possible ways to enhance efficiency in the exchange of police records, system feasibility and impact, four (technical) options were considered that could ensure distribution and exchange of information:

1) No new system/use of existing systems (baseline scenario);
2) Semi-central system;
3) Central system;
4) Decentralised System.

Member States were invited to provide feedback on the business needs and the preferred option from a technical and organisational point of view. They were also requested to provide input on the data needed in relation to the exchange of police records related information and to provide feedback on other system requirements related to data search capacities, system access and data protection.

Stakeholders had different views on the potential added value of a new EPRIS system for the daily operations of criminal investigators and police officers. But the survey and interview outcome has shown that the majority of consulted EU law enforcement experts do feel that there is a need to improve the efficiency of the process to determine in which EU Member State(s) more information on a suspect can be found. But opinions were quite diverse as to whether or not there is currently a need for a new specific EPRIS instrument.

The study has identified the following law enforcement needs in relation to the exchange of police records related information:

- The exchange should take place in the context of criminal investigations;
- The main objective of improving the information exchange would be to improve the process of hardening/verifying a suspicion based on information from other EU Member States (strengthen the case/find additional proof);
- Criminal Investigation Officers and officers performing criminal investigation activities of the Border Guard or Customs services should have direct access; however a gradual approach is preferred, police officers only having direct access in the first phase;
- There is no need to use fingerprints to search in a new system;

- Transmission of information on suspected persons and perpetrators (labelled as guilty by law enforcement authorities) only should be facilitated;
- Additional information should be exchanged in addition to hit/no-hit information to provide a better understanding of received information;
- The answer on which EU Member State holds the requested information should be received within 2-4 seconds;
- The police records exchanged within the system should be restricted to records related to a limited number of offences only.

The study has shown that there are several already existing systems in place which could serve the business needs and purposes EPRIS is aiming at. Most importantly, several Member States stressed the fact that the technical and legal framework of the Europol Information System could in fact address the most important business needs in this context. But on the other hand, the scope of the Europol mandate excludes some offences and the system is not used to its full potential and clearly contains insufficient information at this moment. When it comes to the purpose of allowing law enforcement authorities to alert their European colleagues if a certain individual is considered dangerous, the Schengen Information System (SIS II) could be used. If fingerprints and DNA data is available for a person, the Prüm information exchanges will allow officers to check if police records are available in other EU Member States given that the Prüm system is fully implemented and that the quantity and quality of fingerprints and DNA data in the national information systems will be sufficiently high.

The analysis has thus revealed that the existing systems might address the business needs partially but also that there is no single system that addresses the business needs examined in the context of this project in a comprehensive manner for the moment. If a decision would be taken to cover the existing gap by establishing additional functionalities or a new IT system now or at a later stage, a clear preference for a decentralised storage of data at EU was expressed. Such an approach is in line with the principle of subsidiarity, allowing the principal data owner, the Member State authority, to retain control over the information directly and manage the creation, editing, updating and deletion of data.

The assessment of the user needs and the comparison of different options under consideration, have led to the following recommendations:

- To maximise the use of the existing systems and tools by taking concrete actions at EU and Member State level which take into account the identified business needs and are capable of fulfilling them, in the first instance, particularly regarding EIS and SIENA, Prüm and SIS II. This will allow for an improved exchange of police records related information without major investments in new technical solutions or disruptive changes in the existing legal framework. This involves providing stronger incentives and a closer monitoring of Member States to abide by their obligation to share police record information with their European counterparts via the Europol Information System (using five data fields as a minimum and allowing for the use of the Europol Information System as a hit-no hit system).
- To ensure a sound, continuous and transparent evaluation of progress made with respect to data upload and the use of the Europol Information System during the next three years.

If the need for a more efficient exchange of police records related information is not fully addressed by the better use of the existing systems and tools in the course of three years, then a pilot project should be initiated with the aim to evaluate the technical feasibility and impact of a new, specific EPRIS system. This study outlines the following suggested features of a new semi-centralised system based on the impact analysis and stakeholder preferences:

- Limited central management but no information stored centrally, at EU level.
- A central forwarding system relays queries from requesting countries to receiving countries.
- Information from a limited number of data fields (name, surname, nationality, date of birth, sex, type/date of offence) from existing national law enforcement databases are extracted and converted to a standard EU format into an EPRIS national database that is managed and controlled at Member States level.
- Hit-no hit queries launched from one Member State are executed in all EPRIS national databases. The EPRIS query system is triggered automatically by a query in a national system or after selection by the users.
- The consolidated query response provides a list of "hits", enlisting Member States where information on the queried individual is available together with contact data of the national contact point and categorised information concerning the offence type for which an individual has been suspected and the date of the offence. The system also enlists Member States for which there was no response to the query or produces a general, consolidated response that "no information was found" for all EU Member States.
- After a hit information, bilateral information exchange accompanied by a clear statement of the purpose of the information request takes place between the national contact points.

Any investment in a new specific system or existing systems is an investment to fight crime and to reduce the costs of crime.

2 Introduction

2.1 Background

With the increasing prevalence of cross-border crime in the EU and due to its serious nature, improving exchanges of police records related information has been a priority objective set in a number of legislative instruments[1]. The EU acquired yet more competences in strengthening police cooperation and fight against international crime with the adoption of the Lisbon Treaty.[2] However, whereas EU instruments adopted so far in the area focus on procedures of information exchange, there is currently no exhaustive regulation governing the establishment of whether the required police information exists at all. A number of studies conducted at EU level in recent years[3] confirmed that even though being numerous, the current mechanisms for law enforcement information exchange often do not answer the existing needs.

As a possible solution to this existing gap, the proposal to establish a European Police Records Index System (EPRIS) was put forward which would enable the law enforcement services to check if other Member States hold police records information on a person in question. According to the Stockholm Programme,[4] the European Commission was called on to *"make a feasibility study on the need for, and the added value of, setting up a European Police Records Index System (EPRIS) and to make a report to the Council in the course of 2012 on the issue."*

Police officers throughout Europe strive to respond to the needs of (potential) crime victims. They visit crime scenes, follow up on crime reports, work on identifying and apprehending the persons responsible for criminal acts, and recover stolen property and evidence. Moreover, they often play an integral part in the prosecution process ensuring that suspects are charged with an offence when sufficient evidence is found.

The total number of investigating officers throughout the EU is substantial. Eurostat statistics show that the total number of police officers amounts to almost 1.7 million officers in 2008 (an average of approximately 60.000 officers per Member State). Not all police officers are involved in criminal investigations but this number also excludes staff from other authorities who may be involved in investigative work. Throughout the EU, investigating officers may work for a national or regional police force, but also for customs or border guard authorities if they are mandated by national law to detect, prevent, investigate or prosecute criminal offences.

[1] The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53/11 of 03.03.2005; Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386/89, 29.12.2006; Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, *OJ L 210, 6.8.2008*

[2] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306 of 17.12.2007

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

[4] The Stockholm Programme - An open and secure Europe serving and protecting citizens, 5731/10, 10.03.2010

There is a strong interest of investigators in an efficient international information exchange, especially with regard to cases that may have international implications. However, one of the challenges in this context is that the investigator, in most cases, does not know with certainty whether an individual is internationally active or whether there is any criminal investigation records related information on a person in question, and if so, in which country it exists. Interviewees also pointed to the fact that local investigators are often unaware of, or underestimate, the potential value of police records that might be available in other EU Member States.

Investigations almost always involve gathering information of some sort, interviewing parties and collecting evidence motivated by criminal justice finality. By developing and maintaining active relationships between different local, national and international law enforcement agencies, investigators throughout the EU successfully bring criminal cases to prosecution and conclusion.

Both the efficiency as well as the confidentiality of the information exchange are therefore critical success factors of investigative work and there is clearly room for improvement in this regard. In January-March 2010, a pre-study on the need for, and the added value of, setting up a European Police Records Index System (EPRIS) [5] was conducted which revealed that the majority of the participating Member States (13 out of 16) confirmed the need of an EU action to improve the exchange of police records. However, the interviews and responses in this project have also shown a wide divergence of opinions as to which concrete actions are necessary. Moreover, the 2010 Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments[6] pointed to a somewhat contradictory finding that for many stakeholders the existing legal and technical instruments are broadly sufficient and that they see no strong need to introduce new instruments for cross-border information exchange.

In October 2011, the Commission tendered a study on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records Index System (EPRIS). Its main objective was to investigate the need and possible approaches, in particular the establishment of a European Police Records Index System (EPRIS), for identifying whether police records related information is available in one or several EU Member States.

This report aims to present the final results of the study based on the outcome of the consultation with experts at national and EU level. The main source for evaluating their preferences was answers to the study questionnaire as well as mission reports summarising the findings of visits to 12 Member States (see *Annex 7: Main study instruments*). In addition, the feedback received during the different expert meetings and additional research conducted by the study team formed a significant part of the analysis. The report concludes by presenting the recommended approaches for the future information exchange between law enforcement authorities in EU.

2.2 Study Objectives

The study had several below presented objectives:

[5] Conclusions of Council Ad Hoc Working Group on Information Exchange: European Police Records Index System - elements for a pre-study, 15526/2/09 REV 2 CATS 116 ENFOPOL 282, 21.12.2009

[6] ICMPD and EPLO 2010: Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments

- to analyse ways of providing a definition of the term "police record" at EU level and to propose a common terminology of a “police record” at EU level;
- to look into the reasons why there is a need for information existing in one EU Member State's police records to be available for other Member State(s);
- to examine the organisational structure of and information contained in the national police records databases in 27 EU Member States;
- to provide a description of the data related to police records which should be contained in such a European index system;
- to examine, describe and evaluate different options for possible IT architecture solutions for a hit/no-hit system and an index system;
- to describe the main difficulties to be resolved to achieve the construction of the European index system and the appropriate interconnection with it.

2.3 Methodology

The approach taken to conduct the present study consisted of four complementary elements:

- *Desktop research*, which included the review of the current legal framework, relevant studies and other documentation in the field;
- *Project guidance*, taking place through subject matter expert meetings providing strategic advice;
- *Member States consultation*, consisting of collection of national experts’ and practitioners views and preferences for the future mechanism;
- *Consolidation and analysis*, which represented the evaluation of the existing systems/tools and implications that the proposed solution(s) would have.

It is important to note that the targeted authorities of the study were the law enforcement services dealing with criminal investigations. More specifically, it concerned prevention, detection, investigation and prosecution of criminal conduct and did not include administrative policing.

For study methodology details, see *Annex 2: Methodology.*

2.4 Difficulties encountered

In the course of the study, several difficulties were encountered which are briefly summarised below:

- Due to the difficulties in defining the responsible competent authority, the nomination of a SPOC for the purpose of the present study was delayed in several cases. Such situation implied additional efforts of the study team to ensure the continuity of the communication on the subject matter.
- The second difficulty encountered by the study team, which in some cases was caused by the late appointment of the SPOC, resulted in delays in returning the completed study questionnaire. Several reminders were sent and telephone calls were made to speed up the process after which responses from all 27 Member States were received and incorporated in the analysis of the present report.

- Due to the above described difficulties and time constraints imposed by the tight schedule, strong efforts were required to manage the mission planning in order to have twelve Member States visited within the agreed timeframe. All missions that had been foreseen were successfully completed.
- During the study visits, several stakeholders expressed their concerns that performing a more detailed assessment of possible approaches may only take place when fundamental choices have already been made. The study team therefore focused on gathering the business needs rather than discussing the detailed architectural possibilities. The business needs overview is included in section 3 of this report.
- A considerable number of Member States' experts were not able to provide quantitative responses. This led to a limited amount of data related to the number of national queries, international exchanges and implementation costs of relevant systems. The study team conducted additional research to provide further insight into the impact, costs and benefits of the proposed solution but estimates should be interpreted with caution.
- Participants to focus groups meetings repeatedly insisted that the determination of the most appropriate approach implies making political choices. The study team took their observation into consideration while remaining neutral in providing the results of the study.
- Flexibility was required from the Study Team to adapt the methodology to the evolving mission objectives throughout the course of the study within the boundaries of the contract.
- Proposing different options for the term "police records" did not seem opportune as most Member States indicated there needed to be a discussion related to the need for an EPRIS system first, before starting a more detailed comparison of several police record definitions. The study methodology was adjusted to ensure a more fundamental assessment of the need to have a common definition, resulting in the proposal of one definition and related recommendations based on feedback from Member States.

3 Business needs

3.1 General user needs

When asked in the questionnaire to describe the most typical scenarios in which an authority dealing with criminal investigation needs access to information contained in records from other EU Member States, law enforcement experts pointed to the following use cases.

Use case types mentioned in the questionnaire	*Nº MS*
Find relevant background information on the suspect/criminal organisation for further investigation, link with other crimes, criminal history, previous convictions…	19
Link suspects/criminal organisations with other objects (vehicles, telephone number, e-mail, weapons, drivers licence, …)	12
Confirm the identity of a suspect	8
Find information on similar cases in other EU MS (e.g. bank robbery by unknown persons but looks like x with use of object y and z)	8
Confirmation of the identity of a suspect (in the field)	3
Find information on companies and their presence in non-police databases (e.g. to control if they pay VAT, are registered, …)	2

Table 1: Use case types mentioned in the QST

The used case types enlisted in the above table do not imply however that the list is exhaustive and that a new EPRIS system would necessarily be needed for aforementioned business needs. During the missions to the Member States and the Expert Meeting on EPRIS in Brussels, the general list of user needs became more comprehensive. However, the discussions have also shown that for most of these needs, existing EU systems might suffice under the condition that they are fully implemented and used to their full potential. Such observation may be well illustrated by the list of additional user needs summarised in the table below.

General user needs expressed	*User feedback*
Knowing whether a person is dangerous	This need may be addressed by SIS II when implemented.
Determine identity if the identity is unknown Confirm identity if the identity is uncertain	This need may be addressed by Prüm under the condition that it is fully implemented and that the quantity and quality of fingerprints/DNA/vehicle registration data in the national information systems is sufficiently high. The Prüm framework does not allow for automated searching on photographic material. However, SIS II has the ability to carry photographic material – when part of an alert; thus, this need may be addressed by SIS II when implemented.
Find suspect(s) based on information related to events/objects	SIS II has the ability under Art 36 SIS II Decision to search for vehicles, boats,

	planes, containers linked to serious criminals. Also, links may be established between alerts of different categories – wanted person-stolen vehicle; thus, this need may be partially addressed by SIS II when implemented.This may offer potential in the long term. However, currently EU law enforcement authorities did not express a strong need for new functionalities or a new system offering this capability at EU-level as there are more important other priorities.
Discover good practices to tackle a certain crime phenomenon (best practices)	This may offer potential in the long term. However, currently EU law enforcement authorities did not express a strong need for new functionalities or a new system offering this capability at EU-level as there are more important other priorities.
Hardening/verifying a suspicion based on information from other EU Member States (strengthen the case/find additional proof)	**The large majority of MS stressed this as the most important current criminal investigation business need. This would be the most typical use of any system that allows law enforcement authorities to identify whether information on a certain person required for criminal investigation purposes is held in (an)other EU Member State(s).**

Table 2: General user needs

The survey and Member States interviews have confirmed an overall business need for low cost solutions characterised by simplicity and flexibility and a need to avoid profusion of different information exchange channels as much as possible as they may lead to confusion for law enforcement officials. Some interviewees also pointed to the need to limit unnecessary information overload. Weeding through a large quantity of information can be burdensome, costly and even risky when it means that important information is overlooked.

Any information, even hit/no-hit information, should enable the investigator to take a decision, even if this is just the decision to request more information from another EU Member State and wait before taking a decision at national level. Additional qualitative and reliable information from other EU Member States may, for example, play an important role in making the following law enforcement decisions:

- Do I engage in a pursuit of this person?
- Do I hand out a replacement document in case of lost passport or ID-card?
- Do I take coercive measures?
- Do I investigate this person (further)?
- Do I perform a (more profound) house search/vehicle search?

- Do I arrest this person (detain this person longer)?
- Can I find out who (else) is associated with this crime/person?
- Do I obtain a search/arrest warrant?
- Do I order wire-tapping?
- Do I charge/prosecute this person?

Hit/no-hit information or hit/no-hit information with a limited amount of additional information (such as the offence type and date of offence) does not suffice to take measures but it may suffice to take a decision to investigate further and not to close the case.

When asked in which phase of the investigation the information clarifying whether criminal investigation records are available in (an)other EU Member State(s) would be particularly useful, many law enforcement authorities stressed the fluidity of the investigative process and the fact that this information could be useful at any moment. However, some Member States pointed to a more particular need for this information at the start of an investigative process. That would be the moment where an investigator is not sure yet whether the case has international implications or whether criminal organisations might be involved. It would also be the moment where a more comprehensive overview of existing records might lead to a much shortened investigation process. Information related to previous convictions (criminal records) stemming from ECRIS only is likely to be insufficiently timely for investigative purposes as the judicial process and registration of a criminal record may take several years.

3.2 Relevance of existing systems and tools

Experiences of the last ten years have shown that the assumption that existing systems are used to their full potential should be not taken for granted. Interviews in this study confirmed previous findings that a large majority of EU Member States greatly underuse the capacities of the Europol and Interpol information system and the EU Customs File Identification Database (FIDE). This is not due to legal constraints, but to a lack of motivation and national capacity to provide information which may be of use to other EU Member States. Criminal investigation information is, by its very nature, sensitive so there are good reasons to exchange this information with caution. However, legal and technical safeguards exist and can be strengthened further. Providing access to national police information is an investment that provides benefits to other EU Member States and, understandably, such investments are not seen as a priority in most EU Member States. EU-level financing schemes might be useful in this regard. Existing legal obligations alone, such as the obligation to upload information to the Europol Information System (EIS) have not been an effective motivator so far.

Financial, technical or political obstacles aside, police officers throughout the EU need timely, accurate and relevant information. They do not need empty or low quality (existing or new) databases. As rightly stressed by one of the national delegations participating to the EPRIS Expert Meeting, databases or communication systems are only as good as their input.

Some experts have stressed the need for greater access to different types of data or information systems; such as EURODAC, EU-PNR and, in particular ECRIS data. Interpol is also considered a very useful system allowing access to data from non-EU countries. However, four EU systems seem to offer the most potential to address the need of law enforcement authorities to identify whether information on a certain person is held in (an)other EU Member State(s). The following table provides an overview of these systems.

Relevant Systems Overview				
System/ tool	***Purpose Definition***	***Data stored***	***Access to data***	***System limitations***
EIS	To support MS' competent authorities in preventing and combating **organised crime, terrorism and other forms of serious crime** affecting two or more MS	Data on persons **suspected of crimes** falling under Europol's mandate (personal data including biometric identifiers, convictions, and organised crime links)	**3516 users**; this number is expected to increase in the coming years, because only since the beginning of 2012 it is possible to make the EIS available to competent authorities on a hit/no hit basis	**1. System underused** (not equivalent amount and quality of data per MS) **2. Limited scope** of Europol mandate **3. Limited access** and the possibility to query the system in MS
SIENA	To provide a **secure way** to manage the exchange of **operational and strategic crime-related information**	Serves MS as a relay and messaging service between MS **without storing** the content of the information	**Around 3000** users with increased extension to competent authorities and the direct access for strategic and operational cooperation partners	**1.** Currently offered as a web based form that **cannot be integrated easily** in MS systems (also due to EU RESTRICTED accreditation) **2.** Most activities necessary for EPRIS' purposes require **a manual intervention**

SIS II	To **ensure a high level of security** within the Schengen area, including the **maintenance of public security, public policy and the safeguarding of security.** Also to apply provisions relating to **the movement of persons** within the Schengen area using information communicated via the system	Alerts on **wanted/missing/ sought persons and objects** and on **persons and objects** posing **threats to public security**	**Large group of users:** MS authorities responsible for border control and other police and customs checks; by extension - national judicial authorities. In case of a hit, the local SIRENE office is involved in each country (10-60 people per MS). Also, authorised staff of Europol and national members of Eurojust and their assistants	**1. Not yet operational** even though SIS I could be used to cover some of the needs) **2.** Sometimes erroneously perceived as simply a border control/migration instrument although this is not borne out by the legal instruments nor by the information within the SIS which is largely law enforcement based. **3**. Lack of data on **persons or objects known**, if they are not currently wanted/missing/sought or presenting a threat to public security
Prüm	To improve cooperation between EU police and judicial authorities **to combat terrorism and cross-border crime more effectively**	Anonymous DNA and FP, VRD information on **individuals suspected of criminal offences**	**Limited group of users:** contact points transmit requests; domestic access is governed by national law	**1. Not operational** in all MS **2. Lack of person/object related data other than** DNA/FP and VRD

Table 3: Relevant systems overview

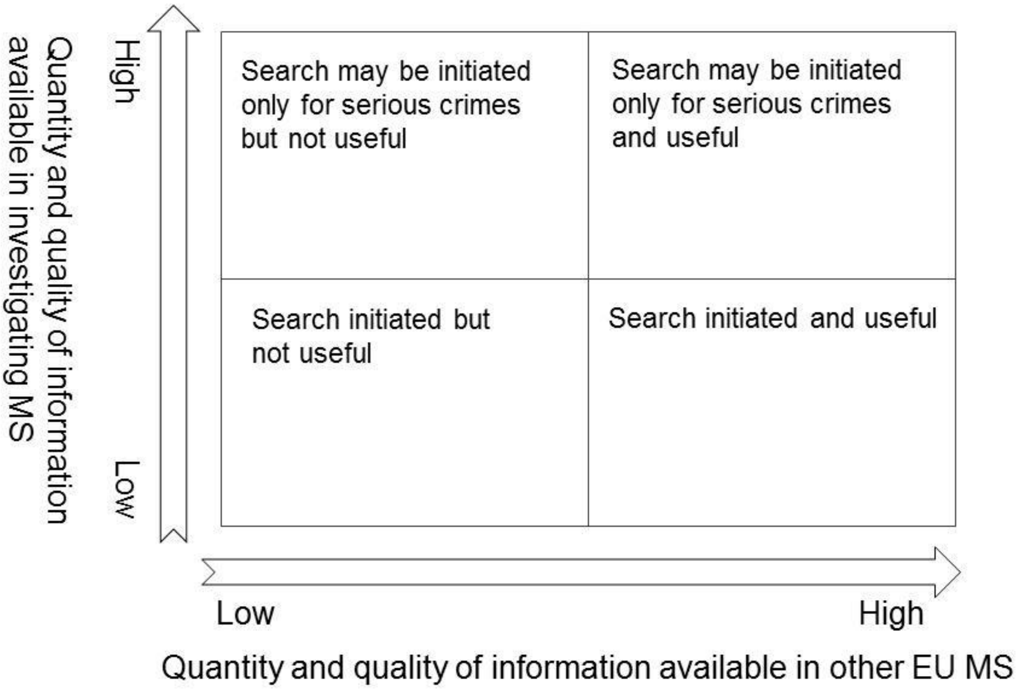
The column regarding current system limitations clearly shows that existing systems might address the business needs partially but there is no single system that addresses the business needs examined in the context of this project in a comprehensive manner for the moment.

3.3 Information query and exchange needs

Member States have selected quite a broad range of information types to be used as search criteria in a system supporting the identification of police records throughout the EU (with an average of 17 out of the 35 provided search criteria options considered necessary). The main reason for this seems to be that there is a large variety of use scenarios under consideration. Any piece of information is deemed potentially useful in a criminal investigation.

The actual usefulness of a comprehensive overview of EU police records information depends on the characteristics of a particular case. These characteristics also have an impact on the perceived potential usefulness of an international query which in turn might have an effect on the number of international queries that takes place in practice.

The following matrix provides an illustration of the usefulness of an information query and response depending on the quantity and quality of information available in the investigating Member State (a known factor) and the quantity and quality of information available in other EU Member States (an unknown factor).


Quantity and quality of information available in investigating MS
High
Low
Low
High
Quantity and quality of information available in other EU MS

Search may be initiated only for serious crimes but not useful	Search may be initiated only for serious crimes and useful
Search initiated but not useful	Search initiated and useful

Figure 1: Usefulness of information query and response

In minor crime cases where there is a lot of relevant information available on a certain individual in the investigating Member State, the additional value of extra information from another Member State might be very limited. For serious crimes however it may definitely be worthwhile to check for additional information as it may substantiate the evidence-base or uncover links with other criminal organisations or terrorist activities.

The matrix illustrates the fact that any EU system and EU information value rises for cases characterised by a:

- High degree of urgency to obtain information from other EU MS;

- High degree of dependency on information from other EU MS.

For criminal investigation purposes, Member States experts have stated that there would be no need for a query system with response times of less than 2 seconds at this stage. For bilateral communication, expected response times outlined in the Swedish Initiative seem to suffice:

Expected response time for international requests for information in the context of an investigation	***Description***
Within 2 - 4 seconds	Time span in which law enforcement authorities would like to know in which EU Member State more information can be found
Within 8 – or maximum 72 hours	Maximum response time for an information request based on the Swedish Initiative Framework – priority request[7]
Within one – or two weeks	Maximum response time for an information request based on the Swedish Initiative Framework – standard request[8]

Table 4: Expected response time

Because current EU databases or hit/no-hit systems are insufficiently used or not implemented yet, there is insufficient statistical information about the number of individuals that are registered in more than one criminal investigation records system throughout the EU. These EU-level statistics can only be produced in a reliable manner when the Europol Information System or a specific new EPRIS system would be used to its full capacity.

Current estimates of information queries at national- and international level, however preliminary they may be, can provide a rough indication of police records information needs throughout the EU. The following table presents some relevant figures and estimates:

Proxy indicator	***Description***
Offences recorded throughout the EU in police information systems in one year (2008)[9]	28.5 million
Total number of police officers in the EU (2008)[10]	1.7 million

[7] Article 4(1), Article 4(2), Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386/89, 29.12.2006

[8] Article 4(3), Article 4(4), *idem*

[9] Eurostat figure

[10] *idem*

Average number of queries for police record information by national police officers in the national police information system	*Unconfirmed estimate:* Approximately 200-700 queries per police officer per year (approximately one query per police officer per day)[11]
Total number of queries in national police information systems throughout Europe	*Unconfirmed estimate:* Approximately 1 million – 3 million queries/day across the EU
Average number of international requests for police record information	*Unconfirmed estimate:* The volume of current international police information exchange procedures ranges from 10.000 to 50 000 per year per Member State. Some Member States are not able to assess the volume of exchange as they do not keep statistics in that regard. One Member State assessed that almost 2/3 of the information it exchanges in the framework of police cooperation with other Member States is related to police records.

Table 5: Information needs estimates

3.4 Information system requirements

This section includes the analysis of specific user needs expressed by the Member States concerning a system supporting the identification of police records in other EU Member States in the context of criminal investigations conducted by law enforcement authorities.

3.4.1 Search criteria

3.4.1.1 Person related information

For identifying whether information on a certain person required for criminal investigation purposes is held in other EU Member State(s), first name, surname and date of birth were considered to be necessary search criteria by all responding Member States.

The following person related search criteria were also considered very important by a large majority of the respondents:

Person related information	*Considered necessary by*
Photo/facial recognition	22 Member States
Gender	23 Member States
Alias	21 Member States
Residence or known address	20 Member States
Nationality	19 Member States
Place of birth	18 Member States
Surname at birth	

Table 6: Person related information perceived as important search criteria

[11] Rough estimate based on German and Spanish figures of national police records consultation.

The following table shows the responses related to the perceived necessity of biometric data for the EPRIS system.

Biometric data	***Considered necessary by***
Photo/facial recognition	22 Member States
Personal identifiers such as scars, marks and tattoos	21 Member States
Fingerprint image	16 Member States
Fingerprint template	12 Member States
DNA	11 Member States
Palm prints	11 Member States

Table 7: Necessity of biometric data

The table shows that photo material and other personal identifiers are considered very useful by EU investigation practitioners.

Little over half of the responding Member States support the use of *fingerprints* to search in EPRIS according to the competencies provided by the national laws. After all, search on biometric data allows for most reliable identification of persons and alphanumeric data does not confirm with absolute certainty whether a person of interest in one country is the same as the person in another country. It is therefore considered necessary to allow for the exchange of fingerprint information during investigations. In addition, fingerprints can also enable field police officers to check the identity during standard police procedures.

But several Member States have added strong caveats or have suggested that there is no need to use fingerprints to search in EPRIS. They point to the need for a system providing complete certainty about the legal purpose for which fingerprints have been retained, the need for experts to confirm the hit and the fact that there are substantial costs attached to this type of information. In addition, the Council Decision 2008/615/JHA MS of the EU will automatically exchange fingerprints and DNA information between National Contact Points in the context of Prüm. That is the main reason why there are quite some Member States who see no need to exchange this type of information within EPRIS. For controls in the field fingerprints are not considered necessary. They can be made available through other channels or using other tools (Prüm, SIENA, Interpol or SIRENE) in a second phase.

It was also noted that fingerprints are generally only available if a person has been convicted (of a relatively serious offence) and that it might be counter-productive to limit cross border information searches only to those for whom fingerprints are available.

It was stated that EPRIS should be not an identification system, but a system to find out whether there is a police record on an individual in another Member State.

3.4.1.2 Legal person related information

The following table shows the responses related to the perceived necessity of legal person related information searchable within the EPRIS system:

Information type	***Considered necessary by***
Legal name	23 Member States
Address of registered office	17 Member States
Country of incorporation	
Register and/or number of legal person	
Shortened name/common name	15 Member States
Name of legal representative	13 Member States

Table 8: Legal person related information

The large majority of Member States consider the legal name necessary. Most Member States also feel that the address of registered office, the country of incorporation and the registration number are very valuable information in the context of criminal investigations.

3.4.1.3 Objects/events related information

The following table shows the responses related to the perceived necessity of the most requested objects/events searchable within the EPRIS system.

Information type	***Considered necessary by***
Type of offence	23 Member States
Date of offence	
Vehicle registration data	22 Member States
Firearm information (type/serial number)	19 Member States
Criminal records information (prior convictions)	
Place of crime scene	18 Member States
Type of drugs	16 Member States
Telephone number	

Table 9: Objects/events related information

These responses are very much in line with the information available at national level and currently contained in EU records information system(s) used for criminal investigation purposes by police and other law enforcement authorities.

One of the respondents noted the fact that vehicle registration data will be available within the framework of Prüm as a reason not to include this type of information in EPRIS.

The fact that prior convictions are considered an important investigative element points to a strong business need of law enforcement authorities for the information exchanged within the ECRIS system.

3.4.1.4 Manual searches v automated cross-checks

The majority of Member States (19) have indicated that EPRIS should not only allow for manual searches. It should also include the possibility of ***automated cross-checks*** (i.e. warning you automatically whether or not there is a hit in EPRIS on the data you have inserted in your own records information system). Whereas 8 Member States have indicated that search should be limited to manual searches only (i.e. warning you whether or not there is a hit on the data used to perform a direct query in EPRIS). The clarifications seem to point in the direction that this choice mainly depends on its feasibility in terms of costs and technical complexity. One respondent suggested that this is a rather complex functionality from a legal and technical viewpoint that should not be implemented in the first phase because that might be too ambitious. Moreover, if automated cross-checks do take place, adequate follow up procedures will be necessary. That may prove to be quite costly.

3.4.1.5 Search based on combined criteria

A large majority of Member States (23) have indicated that search based on ***combined criteria*** in case of the multiple hits should be possible, putting the following arguments forward:

- It enables a narrowed down search, quicker and more precise checks in databases, more complex queries and it means obtaining hits for different areas in accordance with entered indicators;
- It would be a safer, more reliable and more integrated search that allows for a better risk analysis and evaluation;
- It would enable users to filter down the multiple hits.

Some Member States pointed to the fact that it is a necessity, not a mere choice, stating that searching must be carried out by a combination of different mandatory criteria in any case (e.g. at least three search criteria such as surname, first name and, if possible, the date of birth, because there is no interest to check only on the first name of a person and a too broad search capacity for a broad range of users is problematic from a data protection point of view).

Functional and operational ease of use is not the only concern however, one Member State has warned in this context that creating a database with a vague or much extended purpose and very flexible searching options would be a violation of database regulations. It was also noted that combined searching might slow down the query process. Four Member States have indicated that they are not in favour of searching on the basis of combined criteria.

Any recommended solution should take the trade-off into account between the need for information on the one hand, to increase investigation alternatives, and the need to keep investments within reason and prevent information overload during standard operations. Some long term investigations might not need much information in the first place but need a good follow up procedure with Member States on a bilateral basis. Obliging officers to weed through several results might not be the best approach. In cases of information overload, a requesting police force may choose not to do the post hit checking for a more minor matter and might even choose not to make the query or data request in the first place.

3.4.1.6 Categories of persons on which EPRIS should be searchable

The large majority of Member States have expressed their preference for including ***suspected persons*** *and* ***perpetrators*** (labelled as guilty by law enforcement authorities) in the scope of EPRIS. Even though there was an equally large number of Member States who has indicated that ***convicted persons*** (found guilty by a judicial authority) should also be included, there were respondents stating that this should not be the case because information on convicted persons and detainees are already included in ECRIS. Less than half the respondents have indicated that EPRIS should be searchable on the categories of witnesses and victims. As for detainees and associates, responses were more ambiguous.

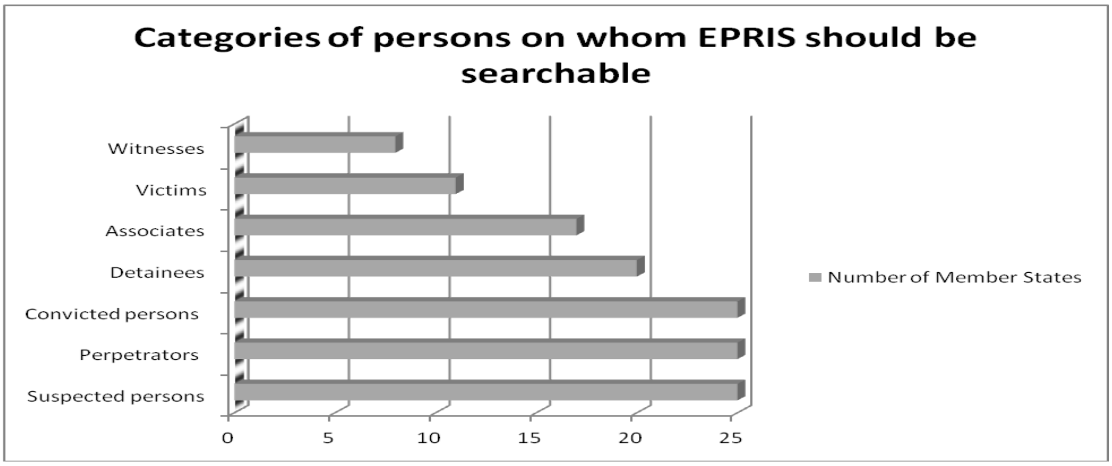


Figure 2: Categories of persons searchable via EPRIS

3.4.2 Information available through EPRIS

3.4.2.1 Hit/no-hit v additional data

In reply to the question whether Member States prefer to receive information as hit/no-hit information only[12], 70% stated that ***a pure hit/no-hit system would not suffice.*** For them, further information would be needed to make the system sufficiently useful in practice.

The information on the ***type of offence*** and ***date of the offence*** would allow users to quickly and easily assess whether there is a need to engage in a follow-up procedure to exchange more information bilaterally. Relevant contact information and the relevant file number could speed up the follow-up process.

16 out of 18 Member States who have indicated that the type of offence information should be provided have indicated that the recently developed EU level offence classification system (EULOCS) seems a useful reference system in this context. After all, it would enable one to understand which crime has been committed in another Member State, even though definitions and languages among Member States differ.

One respondent added that specific warnings and remarks about the subject needed immediately (above and beyond those provided by or within the alerts in SIS) could make EPRIS more useful for immediate, operational purposes. Warning signs stating that a person is considered dangerous in one or more EU Member States could protect patrol officers in day to day operations. Other examples include:

- be aware that the person is:
  - armed;
  - violent;
  - a known member of a group of police interest;

[12] A hit could mean the identification of the Member State(s) holding a certain piece of information required for the criminal investigation purpose in the requested Member State.

    - rowdy;
    - involved in organised pickpockets;
    - involved in organised prostitution;
    - involved in organised illegal immigration;
    - drug dealer.
- avoid contact with this person so as not to interfere with on-going investigation;
- check the person for drugs/stolen vehicles/stolen pieces of arts/use of falsified documents etc.

During interviews it was also highlighted that having the additional information of the Modus Operandi (MO) used to commit the felony could be very helpful for police forces to establish links between investigations. The lack of personal data this information contains would not raise data protection issues but it would be challenging to summarise the MO based on a commonly accepted reference system to make sure that the information would be accessible and understandable by all Member States involved.

For the respondents for whom a pure hit/no-hit EPRIS would suffice, the general reasoning seems to be that such option would be most cautious (safe) approach. It would also be the easiest to build and could already serve the purpose of improving the efficiency of investigations.

The figure below illustrates above discussed preliminary findings:

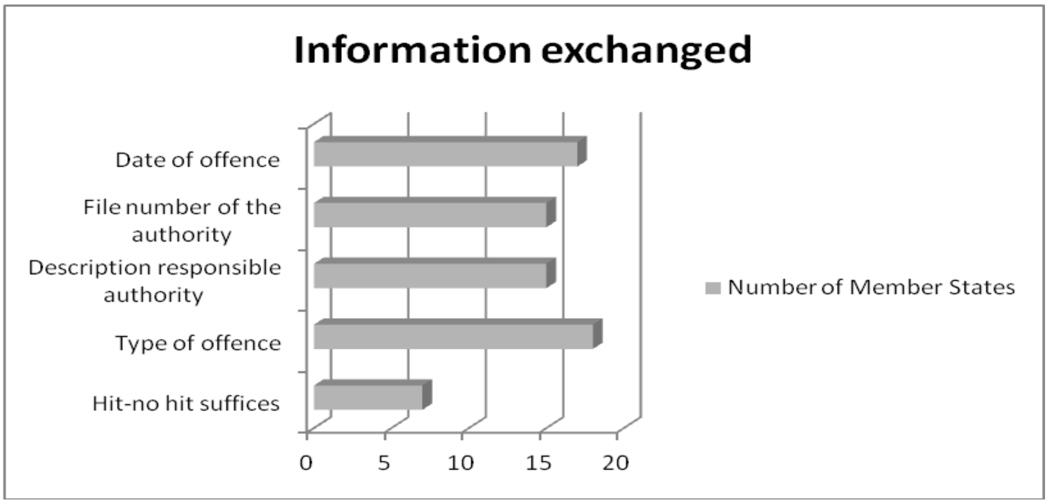


Figure 3: Information exchanged via EPRIS

3.4.2.2 Offence types

Most Member States (16 out of 27) expressed their preference for a European system containing information related only to ***a limited number of offences*** and not to all offences.

Respondents pointed to the offences mentioned in the European Arrest Warrant, (a limited selection of offences from) the ECRIS list, offences falling within the EUROPOL mandate, and those set out in Article 2 of Council Framework Decision 2008/841/JHA as possible relevant classification subsets. Some countries would prefer to make use of a set of offences classified as implying a specific penal severity (possible imprisonment, imprisonment of at least one year). Another option put forward is the use of a simplified list including for instance any sexual, violent and theft offences or other offence types needed to achieve operational objectives.

Re-using reference offence classification systems and data models already in use in other exchange mechanisms would provide great cost benefits and decrease the need for additional interfaces and offence type mapping. Fore-mentioned EULOCS system might be useful in this regard as it has taken the Europol Information System, the Eurojust Case Management System and the ECRIS reference index into account.

3.4.3 System access and use

Member States' experts have different views on the main user group and related optimal design of a system used for criminal investigations. In some countries, patrol officers are seen to play a key role in investigation procedures and a large number of officers are made responsible for initiating and performing investigative activities (a rather bottom-up perspective on investigation work). In other EU Member States, investigations seem to be rather the privilege of more specialised units dealing with criminal investigations (a more top-down approach). These differences in organisational cultures also have an influence on the preferences and expectations with regard to the use and design of a tool identifying whether information on a certain person required for criminal investigation purposes is held in (an)other EU Member State(s).

For the group representing the bottom up perspective, the system of reference seems to be the Schengen Information System used by a large number of patrol officers and providing fast and direct access to information that may be needed during day-to-day operations. For the group representing the top-down perspective, the system of reference seems to be the Europol Information System. This group focuses on making use of existing procedures for the international exchange of police information, and refers to systems in use by a smaller number of more specialised staff with an emphasis on more serious crimes, analytical work and more comprehensive data gathering.

The following table presents EPRIS use projections depending on the different use perspectives:

Query initiation	***Related EPRIS use projections***
Bottom-up initiation of request by police patrol officers if potential link with other EU country	Average of 1-3 million queries/day throughout the EU[13]
Top-down initiation of request driven by political priorities or specialised criminal investigation units only	Much smaller number of queries (e.g. average of 10-50 thousand queries/day throughout the EU)[14]

Table 10: Preliminary EPRIS use projections

[13] Assuming that the number of international requests evolves towards an equilibrium of one third of the number of queries currently taking place at national level. This assumes query initiation for one third of cases, related to all offence types, for all types of persons (EU citizens/third country nationals), in all standard police operation scenarios (including administrative policing). This projection excludes any query initiation by other authority types such as custom authorities or border guards.

[14] Based on current number of international requests, (approximately 50 000/year per Member State) assuming this would rise gradually if an automated system would be in place.

The survey revealed different perspectives from the Member States as to which authority should have access to a system supporting identification of police records throughout the EU. For most Member States, Criminal Investigation Officers and officers performing criminal investigation activities of the Border Guard or Customs services should have direct access. Patrol officers, other authorities and the data subjects should have access through a central authority:

	No Access	**Direct Access**	**Through a central authority**
Criminal Investigation Officer	0	24	3
Border Guard Service/Customs	3	20	7
Patrol Officer	2	12	14
Inspection Service	8	7	9
Prosecution Service	6	9	13
Others (e.g. judicial, penal institution)	9	3	14
Data subject	5	4	15

Table 11: System access needs

Any existing, or new police system should obtain a sufficiently large information- and user base among police officers or otherwise it is destined to fail. Network effects theory states that the added value of communication and information networks grows exponentially depending on the number of users. Critical mass is defined by the type of network an information product operates on, and how many users are needed on that network before the product becomes useful. Users may face various phases ranging from passive usage where there is not enough information to consume, to the point where they are very active and start creating content and uploading information themselves. But the threshold point between the phases is a local observation of critical mass. Several other interrelated theories related to the diffusion of innovation, the bandwagon effect, the tipping point and the one-third hypothesis seem to point towards a minimal user base of one third of the total user group to have sufficient traction.

This implies a target active user base of 600 000 police officers in this context if bottom-up engagement is sought after. It also seems safe to say that EU police record exchange systems should connect to at least one third of the police record information available throughout the EU to be considered sufficiently valuable by officers working at national level. Network theories are not the only considerations however. Data protection and privacy by design considerations are also vital for ensuring sufficient trust in the system. The purpose limitation and proportionality principles are crucial in this regard. The system should target the core objective of preventing and combating crime within the EU. It should be ensured that processes facilitated via EPRIS constitute only a minimal interference necessary with regard to the legitimate aim.

3.5 User needs conclusions

The study has identified the following law enforcement needs in relation to the exchange of police records related information:

- The exchange should take place in the context of criminal investigations;

- The main objective of improving the information exchange would be to improve the process of hardening/verifying a suspicion based on information from other EU Member States (strengthen the case/find additional proof);
- Criminal Investigation Officers and officers performing criminal investigation activities of the Border Guard or Customs services should have direct access; however a gradual approach is preferred, police officers only having direct access in the first phase;
- There is no need to use fingerprints to search in a new system;
- Transmission of information on suspected persons and perpetrators (labelled as guilty by law enforcement authorities) only should facilitated;
- Additional information should be exchanged to provide a better understanding of received information, in addition to hit/no-hit information.
- The answer on which EU Member State holds the requested information should be received within 2-4 seconds;
- The police records exchanged within the system should be restricted to records related to a limited number of offences only.

EU law enforcement officers have confirmed that there is a need to improve the efficiency of the process to determine in which EU Member State(s) more information on a suspect can be found. Whether or not there is a need for a new, specific tool and whether or not it is necessary to construct such a tool at EU level at this moment in time depends on a closer assessment of the different options, presented in *Section 4*. The principles of proportionality and necessity, technical obstacles, cost concerns, access limitations, data control and confidentiality were considered the most important considerations by the large majority of interviewees.

In any case, any solution should take the below enlisted challenges and expert suggestions into consideration.

3.5.1 Challenges

The possible difficulties which might be encountered when designing a new mechanism for police record related information exchange include:

- Existing general resistance to share sensitive data from investigations with a broad audience. This implies that necessary restrictions are needed to limit access on a need-to-know basis. Access limitations and adequate security controls will be required in any solution that is provided. This point will be decisive for Member States to share their data.
- Recent negative implementation experiences with complex large scale pan-European home affairs systems.
- Remaining differences in the levels of technology and human resource capacity throughout the EU.
- Insufficient use of common standards/remaining interoperability challenges/use of different data models throughout the EU.
- Different legal systems and criminal justice terminology interpretations.
- Existing language barriers.
- Use of several different information systems at national level that are not or only partially integrated in some Member States.
- Existing resistance to providing access to other authorities working with criminal justice finality at national level.
- Different data retention rules throughout the EU.

- Data quality differences due to differences in data updating procedures and system metadata[15].
- Possible interconnection challenges caused by differences in the security level of certain information systems or communication channels.

3.5.2 Expert suggestions

- Any investment in a new specific system or existing systems should be regarded as an investment to fight crime and to reduce the cost of crime. Both costs and benefits of any solution should be taken into account.
- Considering current budget constraints, Member States emphasised the need for low cost solutions.
- Existing legal, organisational and technical instruments should be used to their full potential when possible.
- Any new system should be complementary to existing systems.
- Any solution should balance the needs for both security and liberty of EU citizens and suspects alike (considering strong information needs of investigating authorities and the fact that some data is highly confidential).

- Any technical solution should:

  - Be easy to use;
  - Allow for a semi-automated information exchange to lower the costs of information management (with confirmation or validation by national experts where needed);
  - Involve a limited number of data fields for pan-European searching;
  - Have a short response time, but there is no need for response within microseconds; a response within 2-4 seconds suffices.

[15] E.g. some systems do not include a specific marker as to whether or not a person record is a victim or a suspect.

4 Options under consideration

According to the project methodology, four options were considered for the possible development of a European Police Record Index System (EPRIS):

1) No new system/use of existing systems (baselines scenario);
2) Semi-central system;
3) Central system
4) Decentralised system.

A detailed description of each of the option including the key implications in terms of management structure, costs/benefits, legal implications and information technology can be found in *Annex 6: Description of scenarios*.

If a system would be built, preferences revealed the following Member States distribution:

- No preference: 1 Member State;
- Semi-centralised system: 14 Member States;
- Central system: 7 Member States;
- Decentralised system: 4 Member States.

The following tables provide an overview of the supporting and opposing arguments provided by Member States and other stakeholders condulted in the course of the study for the different EPRIS architecture options under consideration.

Centralised	
Supporting arguments	
Argument type	*Specific arguments*
General	One solution for all Member States that's relatively simple and reliable
Financial	Lower financial burden on Member States
	More funding from EU
Legal/data protection	System use can be monitored better
	More control on information provided to requesting country
	More in line with principles of necessity and proportionality
Information management	One question sent to all Member States/optimised querying
	All information is available in one place
	There is only one entry point of contact
	Immediate answer is possible
Technical	Standardisation is easier
	System availability is guaranteed centrally
	Integration is easier
	Quick evaluation tools are available
Organisational	Allows for more efficient management
	Allows for standard policies
Opposing arguments	
Financial	Setting up a centralised database of this nature is a very complex and costly undertaking
Legal/data protection	There are substantial risks to lose control of submitted information which raises data protection and confidentiality issues.
	There are legal obstacles to sharing police record data
	Would create a new database that is not necessary

Information management	Information duplication
	Very hard to set information standards/understand information structures in different countries
Technical	It is too heavy to develop and maintain (with reference to SIS developments)

Table 12: Central system: pros and cons

Semi-centralised	
Supporting arguments	
Argument type	*Specific arguments*
General	Seems to be the best ratio efficiency/cost of implementation
Financial	Medium development, management and operational costs for Member States
Legal/data protection	Minimal need for new legislation
	Better control of data sent to requesting country
	Relevant data is kept with national authorities so data protection can be stricter
Information management	Free manipulation of data at national level
	Communication with one central point
	No duplication
	Potential for a single search
Organisational	No need for new administrative structures
	A single point of contact
Opposing arguments	
General	Considerable administrative and legal work locally regarding thinning of records and legal obstacles of sharing information
	Too complicated
Legal/data protection	No clear feedback on system use
Information management	Input of data can differ in various Member States. This could make the querying difficult or it could result in false hits.
Technical	Complicated system architecture
	Possible failure at central level
	Availability and performance of the system
	Risk of a “central point of failure”
	Requires Member States to build a national index or interface with their own system(s). Existing Member States’ systems might need to be enlarged to handle extra load.
Organisational	Evaluation procedures are complicated

Table 13: Semi-central system: pros and cons

Decentralised	
Supporting arguments	
Argument type	*Specific arguments*
General	This model is already used for Prüm and EUCARIS
	Consistency with most other information exchange instruments
Financial	Less efforts needed (assuming an automated system)
Legal/data protection	Member states retain control over own system and data
Information management	Every Member State can maintain its own database
	No data duplication
	Potential for a single search
Technical	No central failure risk
	Standardised application interfaces have to be developed for system to system communication

Opposing arguments	
General	Strong dependency of the project on political willingness to implement the system, national solution and approaches
	Heavy and burdensome data links between Member States
	Considerable administrative and judicial work locally to thin the records
Financial	Higher cost for Member States because of the use of their own resources for development and maintenance. (Some work might have to be performed seperately in different Member States (duplicate))
Information management	Need to understand information management protocols in different countries
	Slower querying – no immediate response
Technical	In each country there is a need for a solution for every other country
	Inconsistent system availability
	Complex technical solution
	No optimisation of use of bandwith
	More complex to set up
	Standardised application interfaces have to be developed for system to system communication
	Synchronisation issues
	Complex maintenance
	Problems with maintaining connections pair-to-pair
	Certification problems
	Interoperability testing need to take place between all Member States to ensure interoperability with different national systems.

Table 14: Decentralised system: pros and cons

The centralised system seems to have a certain appeal because of its relative technical simplicity. The options with a decentralised component (semi-centralised and decentralised) offer the important advantage that the data is maintained by the data source and data owners, the Member States authorities. Implementation of EU standards (like the UMF2 standard) would be absolutely necessary in this scenario. Responses seem to have been influenced strongly by recent ECRIS, SISII and PRÜM experiences. The semi-centralised option is perceived to offer a combination of the benefits of the other options for most Member States, whereas, for other Member States, this option has the risk of combining the worst of both.

The analysis of the answers to the study questionnaire and country missions revealed that the majority of Member States had a preference for the baseline scenario, the semi-centralised scenario and the centralised scenario for the possible establishment of EPRIS. Corresponding architectural approaches of the three and key considerations are briefly described further below.

4.1 Baseline scenario: No New System/use of existing systems

The baseline scenario corresponds to a situation where no new EPRIS specific system is created at EU level. Apart from preserving the current status quo where no further action would be taken at EU level, this option does include the possibility to improve the existing information exchange and further optimisation of existing systems.

In the study questionnaire, at least 5 out of 27 Member States strongly supported the ‘No New System’ scenario, arguing that existing ways for exchanging information should be looked at in the first place. More Member States were of the same opinion as the study progressed while not excluding the possibility to have additional functionalities based on the business needs in future. Various shortcomings, such as lack of access to the existing mechanisms at national level, a lack of data and low quality of data inputted, were put forward by the experts as obstacles in the current context. Some concrete suggestions on how to improve the current mechanisms were presented by Member States and Europol at the Expert meeting of 19th of April 2012. The interviews and the Expert Meeting revealed that the following systems and tools are considered particularly relevant:

1) Europol Information System (EIS): improving the amount and quality of data uploaded on EIS and extending the access to EIS at national level, automatisation of processes.
2) SIENA: further integrating the tool at national level to address the needs for bilateral data exchange.
3) Schengen Information System (SIS II): using the SIS II technical architecture for exchange of supplementary information (i.e. alerts on ‘known persons’);
4) Prüm: using Prüm mechanism for matching fingerprints, DNA and vehicle registration data.

The baseline scenario *per se* implies that no specific management structure would need to be put in place at EU- or national level, and that no new legal instrument would be required. This applies to a situation where no new functionalities are added and no modifications are made to the current systems and tools. This was the main argument put forward by Member States supporting this option. Moreover, a decision not to develop a new system would also mean that no additional costs would be incurred. In any case, taking full advantage of existing IT channels and legal instruments was considered necessary in any scenario, also by Member States supporting the creation of a new EPRIS system. However, some solutions where brought forward in relation to existing systems that did imply adding additional functionalities or imposing new or stricter obligations to upload data. These options do imply changes at the legal and technical level and may bring about additional operational costs. For instance, a new SIS alert would require a new legal instrument unless operational agreement is sought on better use of discreet check alerts and use of threat assessments to identify the subjects of such alerts. This argument presented by a number of experts at national and EU level deserves further consideration and is presented in *Section 5.2* of this report.

4.2 Semi-Central System

Member States’ feedback demonstrated a clear preference for a semi-central system option for EPRIS. 12 out of 27 Member States advocated for such architectural solution as best fitting the existing needs. The semi-central solution implies establishing a central server only for relying queries from requesting country to receiving countries without storage of data on the server (the hub-and-spoke model). In this scenario, Member States do not send a request to all other Member States directly themselves, they send one request to the central server. Its visual representation is depicted in further below.

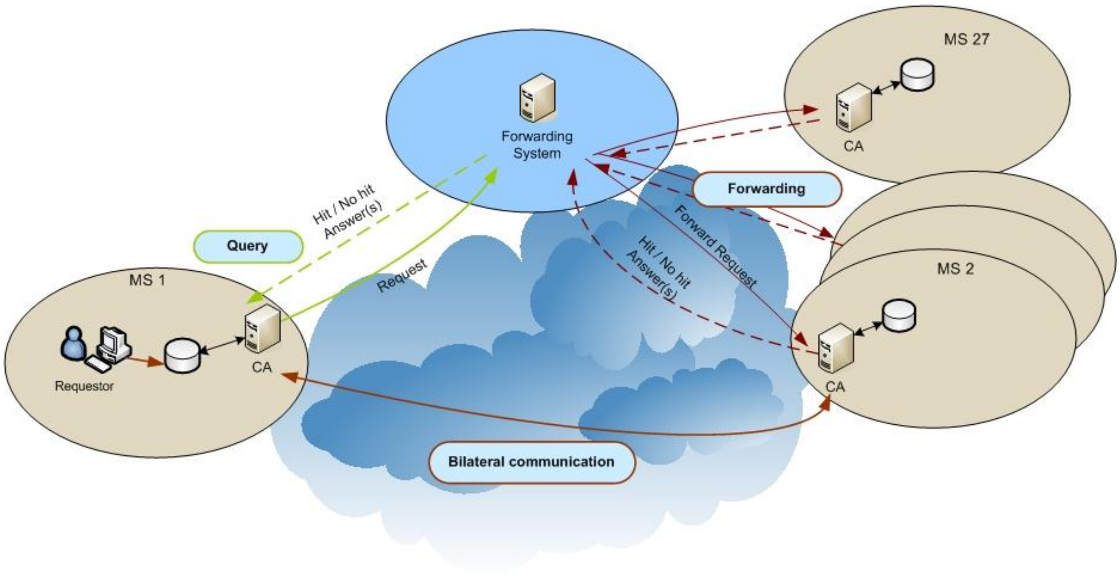


Figure 4: Semi-central system

In this scenario, no data would be stored at the central level. The requirements would include the development of a central relay as well as the connection between the forwarding system and national databases. Also, automated processes should be ensured for handling requests.

Based on the initial description of the semi-central option, Member States supporting this option provided the study team with additional suggestions that were further detailed during the EPRIS Expert meeting. One proposal was to extract data copies from the national police record databases based on five essential search criteria shared by all Member States. According to the Member State's experts, such this solution would help to avoid problems related to the overload of the incoming requests and would ensure compliance with the security requirements. After having searched with five search criteria, the maximum information from other Member State(s) would be received through the bilateral mechanisms ensuring accountability and traceability.

As the semi-central architecture includes elements of the fully decentralised system which in turn found a lot less proponents (supported by only 4 out of 27 Member States), the latter option is not developed in further detail in this report.

4.3 Central System

6 out of 27 Member States supported another solution for the purpose of EPRIS, that of a central index system. As illustrated in the figure below, in this scenario the minimum information necessary to identify a person would be uploaded in a central index established at EU level. Hit/no-hit responses to queries would be provided indicating which Member State(s) should be contacted in the form of bilateral communication for more information. Member States would be required to develop a data conversation and upload tool and integrate the search functionality into a national process and search application (or allow their police officers to make direct use of a centralised search interface).

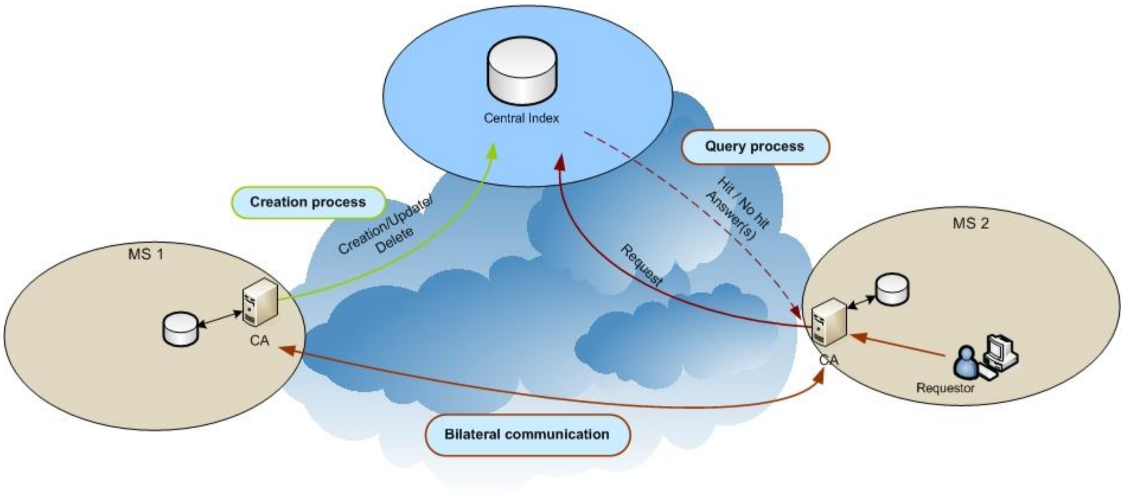


Figure 5: Central system

Apart from the advantages related to the automation of searches, simplified interoperability testing and limited traffic flows, this option has several disadvantages, mainly related to the requirement for Member States to upload information to the system. Centralising data not only raises considerable data protection concerns; the idea of investing in a new centralised system finds very little support because there is already a functioning central database at EU level that allows for hit/no-hit searches, the Europol Information System. This is the main reason why the option of a new, centralised system is not recommended.

5 Recommendations

5.1 Concrete actions – incremental progress

Sharing police information, or providing access to police information via hit/no-hit or direct exchange mechanisms with other EU counterparts requires a constructive EU mind-set from all Member States and stakeholders involved. The enthusiast engagement of study participants has revealed that much progress has been made already. Law enforcement authorities throughout the EU do understand the broader implications of their work and are interested in improving police cooperation. However, the security of EU citizens demands efficient, well-functioning criminal investigative procedures and information exchange mechanisms; action is clearly needed at EU and at MS level to make further progress in this domain.

The Information Management Strategy for EU internal security refers to 'needs and requirements', 'interoperability and cost efficiency', 'decision-making and development processes' and 'multidisciplinary approach' as the main focus areas. Throughout the study, these guidelines were respected by looking into the business needs related to the current law enforcement information exchange and by involving Member States' experts in each stage of the conducted analysis while stimulating interaction between all the relevant law enforcement authorities and organisations at national- and EU level. A high level costs-benefits analysis presented in *Section 5.5.7* of the report allows for an initial assessment of potential cost efficiency of a specific EPRIS system.

Because of the existing business needs highlighted in this report, the current economic crisis, the on-going implementation of SIS II, Prüm and ECRIS, the current lack of data upload to the Europol Information System and the diverging opinions on the most appropriate solution between the different stakeholders, we strongly recommend an incremental, step-by-step and determined approach to improve the efficiency of cooperation between investigating authorities in the EU.

Based on the assessment of the user needs, the broad political and economic context and the comparison of different options under consideration, the following recommendations are made:

1. Recommended actions to improve the use of existing systems and systems currently under development:

   A particular focus on ensuring the full benefits from the potential of the EIS, SIENA, SIS II and Prüm framework is absolutely necessary. This would allow for an improved exchange of police records without major investments in new technical solutions and without the need for major changes to the existing legal framework.

2. A recommended definition of the term "police record" at EU level:

   A common definition may be needed for functional and legal reasons. We recommend a broad definition with limitations specified in system specific legislation, if and when it arises.

3. Recommended actions to monitor and evaluate the effectiveness and efficiency of EU cooperation and EU information exchange with a criminal justice finality:

    The exact social, financial, technical and organisational impact of certain actions can only be assessed after they are implemented on a small scale. Then a sound evaluation of lessons learned can help determining whether the activity should be (dis)continued or expanded to a larger scale.

4. A suggested design of an EPRIS system based on study findings:

    A new EPRIS system might be necessary if important business needs remain unaddressed after the recommended actions related to existing systems are executed (or if they are not executed). The suggested design can form the basis of a pilot project to evaluate the technical feasibility and impact of a new, specific EPRIS system.

These recommendations take into account the broad political and economic context, current practitioner needs and on-going evolutions regarding the exchange of police records related information in the EU area.

5.2 Improved use of existing systems

The study results revealed that the majority of Member States, regardless of whether they supported the establishment of a new EPRIS system or not, confirmed the need for an improved use of several currently existing law enforcement instruments. This finding is in line with observations included in a number of previously conducted studies[16]. The low amount of data inputted, the vagueness of data types and inadequate data quality are the examples of reported shortcomings. Four information systems were selected for a more in depth, recommendation oriented review. Other relevant EU systems are shortly described in *Annex 10* of this report.

5.2.1 Europol Information System (EIS)

One of the most problematic areas related to the EIS is the lack of data uploaded to the system. Whereas different causes were mentioned by Member States experts, including different legal systems, lack of mutual trust or inadequate access at national level, stakeholders' views were unanimous with regards to the need to better use the system to its full potential. Several actions are proposed in order to rectify the existing situation[17].

First of all, it is recommended that Europol formulates guidelines clarifying the obligation to upload data and the sources/databases which should feed the EIS and that these guidelines allow for a broader hit/no-hit use of the EIS (the hit/no-hit functionality in EIS is available since the beginning of 2012). It is proposed that several data fields (e.g. name, surname, date of birth, nationality, type of offence, date of offence) would be selected for obligatory upload, the choice of which can be further specified in the guidelines. As problems related to the data upload and data quality were reported, it would be very useful

[16] ICMPD and EPLO 2010: Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments

[17] See as well Council Conclusions on the increased and more effective use of the Europol Information System (EIS) in the fight against cross-border crime, 7/8 June 2012

if EU financial support is foreseen for improvements to Member States' technical capacity and for efforts made to ensure a more continuous and complete data upload.

Another suggested action that could ensure a broader user base of the system is the extension of EIS access. During the country visits, the study team was informed of projects currently taking place in some of the Member States setting a framework which allows for feeding of the EIS also from the regional level. This can also be stimulated in other EU countries.

Apart from the recommendations above, initiatives to raise awareness on the value of data upload to the EIS (and its update) seems necessary. So does the launch of coordination activities to stimulate the exchange of data upload best practices and tools. Additionally, requests for clarification to those Member States that do not upload the required data should be issued. Finally, the possibility to initiate EC non-compliance procedures should be considered if some Member States do not fulfil the obligations established in the current legal basis.

According to Article 10(1) of the Europol Decision[18], Europol has the legal right to establish and maintain systems processing personal data, this can form the legal basis of further IT support and developments by Europol.

All the above proposed activities fall within the existing legal framework and are thus possible to implement without the need to make changes to the Europol Decision. But additional legislative actions should be considered. First of all, a number of Member States advocating for the establishment of the EPRIS specific system covering all offence types referred to the Europol mandate limitations. Even though some might argue that the crimes list for which Europol is competent is quite wide, practically covering all offences enlisted in the European Arrest Warrant Decision, it still excludes a broad list of offence categories (see *Annex 11* for the full list of offences which formally do not fall under the Europol mandate). The current reform of the Europol mandate foreseen to be finalised by the end of 2012 and is an excellent opportunity to address this gap and include other serious crime types. If the mandate is not broadened then the EIS will not be able to cover all information needs identified in this study. We therefore strongly recommend broadening the scope of the Europol mandate to cover all serious crimes.

Similarly, the introduction of a more specific legal requirement to upload identity data fields for the hit/no-hit use in the existing instrument would strengthen the current obligation to upload data to the EIS. A number of field's experts have expressed their concern that the existing legal obligation can be widely interpreted by Member States due to its relatively vague formulation.

5.2.2 SIENA

Another tool which needs particular attention in the context of improvement of police cooperation at EU level is Europol's secure communication tool (SIENA). SIENA is already used by several Member States allowing for a possibility to exchange operational and strategic crime related information beyond Europol's mandate. With its current

[18] Council Decision establishing the European Police Office (Europol), OJ L 121, 15.5.2009

functionalities, the tool can also serve as broadcasting mechanism, i.e. sending a query to all other EU Member States at the same time.

In order to increase the usability of SIENA among all Member States, several initiatives are recommended, such as the extension of its accessibility to all central units of criminal police. Also, the technical integration of the tool must be encouraged. It is now mostly delayed due to its web based form. Finally, the step-by-step automation of sub-processes related to the exchange of information to support efficient and secure query responses in a (semi-) automated manner should take place as currently most of SIENA related activities/processes are manually driven.

Initiatives to improve the usability of SIENA among Member States are already on-going. Currently a pilot phase is in progress to test an automated message exchange from and to Member States. This automated message exchange would permit SIENA to be used not just as an exchange platform between users, but also between systems.

SIENA is accessible through the Europol network that interconnects the different Europol National Units (ENU). Local law enforcement authorities in turn are connected to the National ENU and can access the SIENA system.

SIENA is thus excellently placed to facilitate information exchanges between Member States, both in a manual and automated manner. Any new systems or existing systems with limited information exchange at the moment would benefit from looking into SIENA as the platform for their message exchanges. By reusing an architecture that is already in place spanning the different police services throughout Europe, creating new information exchanges can be done much simpler and less costly.

It is important to note that, according to the Europol Decision, the agency may facilitate the bilateral exchange of information also outside the Europol mandate. The UMF II tool which used for integration of existing EU standards should also be mentioned in this respect. As a consequence, Europol may provide its automated search services linked to other systems, except for SIS II, which could be rectified by introducing a change in the legal basis. In case of all other systems, a high level of interoperability of services between existing systems and tools has been already made possible and should be made use of to add efficiency to the existing mechanisms.

5.2.3 SIS II

The Schengen Information System is seen as a key instrument established for the purpose of EU’s internal security and migration management. The second generation Schengen Information System (SIS II) will replace the current system, providing enhanced functionalities. Several observations were made by Member States’ experts regarding the systems relevance to EPRIS during the study consultation round. It is thus worth looking into certain parts of SIS II in order to find out whether they could be used for improving the current police related information exchange.

Out of all categories of alerts that will be included in SIS II according to SIS II Decision[19], the alerts on persons or vehicles, boats, aircraft and containers for discreet or specific checks for the purposes of prosecuting criminal offences and the prevention of threats to public security (Art 36 and 37 of the Decision) fall under the EPRIS scope. For this group of serious offenders this alert may already prove useful for the exchange of information EU-wide.

For the time being, it is not possible to interconnect different databases with SIS or to insert a data field "known person" in SIS II (a suggestion made by one of the Member States experts). To allow for this, substantial changes in the legal basis would be necessary. This seems ill-advised considering that the main priority for the SIS II at this stage is to have the system up and running. However, the use of coordinated workflow systems and intelligent search tools allow Member States to manage SIS alerts alongside other channels of information exchange and to search several databases at the same time whilst still respecting data separation.

The main reason why stakeholders did stress the value of SIS as a model is the fact that it is an operational tool providing access to a large user base, including patrol officers in the street. This could be a model for any police record identification system accessible to many in the mid- to long term future, especially as both fingerprints and photographs of alert subjects can be stored in the central SIS II.

5.2.4 Prüm

When asked whether biometric data should be included as search criterion in EPRIS, should the establishment of such a system be agreed upon, respondents gave an almost unanimous answer to use the Prüm mechanism for exchanging biometric data instead. Indeed, the Prüm decision seems to be one of the most efficient tools to identify criminals and solve crimes when interconnecting the vehicle registration, fingerprint and DNA databases of the Member States. This is due to the possibility of almost instantly knowing if a certain type of information is available in another Member State and, if so, where it is kept. Since a formal request can then be sent directly to the appropriate authority via existing channels, such as SIENA, this facility is regarded as enormous value to investigations, gaining time and increasing efficiency.

However, differences between data exchange via Prüm and a possible EPRIS should not be overlooked. First of all, searches in police records are often based on names whereas for Prüm searches DNA or fingerprint profiles are needed (relevant for non-arrested suspects). Secondly, storage criteria for fingerprint data in national databases (which are accessible via Prüm) are certainly different, i.e. more restrictive, than those for national police records. Furthermore, Prüm data are considered judicial data in some Member States which entails the need for judicial authorisation – unlike usual police records data. These observations imply that a comparison between Prüm mechanism and possible EPRIS should be made with caution as in many cases they cannot be considered replacing one another.

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

The implementation of the Prüm Decision[20] has not yet been completed; the Commission's Prüm implementation report (required by Article 36 of the Decision) will summarise the state of play and underline the need to finalise the implementation. In this context, it is recommended to foresee incentives in order to improve the quality of Prüm exchanges throughout the EU ensuring that identification processes are improved. Also, the full use of Prüm for DNA, fingerprints and vehicle registration data by criminal investigation officers should be guaranteed. This would contribute to developing a more coherent approach to the exchange of personal information for law enforcement purposes, referred to in the Information Management Strategy for EU internal security.

5.2.5 Summary

The below table summarises the key points of this section. It provides a short business needs overview and subsequent recommendations for the four relevant systems/tools. In addition, it includes general suggestions to improve overall efficiency and effectiveness of the process of finding out whether another EU MS has any criminal investigation records on a person, such as strengthening the network of national single point of contacts (SPOC), improving overall trust in the data quality of national systems or broadening integration with and access to national criminal records databases, ECRIS and Interpol systems.

Business Needs Overview		
System/ tool	***Business need: Know whether another EU MS has a criminal investigation record on a person, and if so, which EU MS***	***Recommendations to maximise system potential***
EIS	Know whether Europol stores information on a person Know which EU Member State can provide more information related to a record in the Europol Information System	**Within current legal framework:** • Stimulate extension of EIS access to broaden user base • Formulate guidelines clarifying the obligation to upload data and the sources/databases which should feed the EIS and allow for a broader hit-no hit use of EIS (using identity data fields) • Raise awareness on the value of data upload to/update of EIS • Coordinate exchange of data upload best practices/tools • Provide EU financial support for improving technical capacity improving data upload and data quality • Request clarification to Member States that do not upload • Initiate non-compliance procedures if necessary

[20] Council Framework Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L212, 6.8.2008

		With new EU legislation: • Extend Europol mandate to include more offence types • Create a legal obligation at EU-level to upload data and allow for a broader hit-no hit use of EIS (using identity data fields)
SIENA	Provide for a secure information channel to exchange information	**Within current legal framework:** • Use Siena as broadcasting mechanism (sending query to 26 Member States) • Step-by-step automation of sub-processes related to the exchange of information to support efficient and secure query responses in a (semi-) automated manner **With new EU legislation:** • To adapt legal basis so that Europol could facilitate bilateral exchange also outside Europol mandate, i.e. provide automated search services linked to other systems (e.g. SIS II)
SIS II	Know whether other EU Member States hold records on a person signalling that he or she is wanted/missing/sought or presents a threat to public security and providing more details	**Within current legal framework:** • Focus on implementation to ensure public security and safety of law enforcement officials throughout the EU during day-to-day operations
Prüm	Know whether other EU Member States hold a matching fingerprint/DNA or VRD record and confirm identity match. When there is a match, there may also be a criminal investigation record linked with this record.	**Within current legal framework:** • Focus on implementation to improve identification processes
General	Improve efficiency and effectiveness of the process of finding out whether another EU MS has any criminal investigation records on a person	• Further strengthen and integrate national contact point network • Improve collection and analysis of statistics of EU police records exchange to locate potential gaps and overload in information flow • Support use and implementation of common standards to enable (semi-)automated data exchange • Improve trust in the data quality of national systems – set up common data quality evaluation mechanisms • Strengthen fingerprint quality and quantity • Broadening access to national criminal

		records databases and ECRIS - Investigate potential linkage between ECRIS and Europol - Determine EU use of Interpol Information System Strategy/deepen Interpol – EU system integration

Table 15: Business needs overview

Considerations related to other relevant systems such as CIS/FIDE or ECRIS can be found in *Annex 10*.

5.3 Definition of the term "police record" at EU level

The issue of defining the term 'police record' at EU level, referred to in the study objectives, and of the need for such a common definition in general is closely related to the national context. The majority of experts consulted during the Member States' consultation round had no strong opinion on what such definition should include or whether it is at all needed. This may be explained by the fact that at national level, rather than the content of the records, the sharing of this information seems to be regulated. For instance, in some cases, there are limits on the sharing of police information to certain other (national) law enforcement authorities. This can be well illustrated by the following figures:

1) 6 out of 27 Member States do not have a legal nor functional definition of the term 'police record'
2) 14 Member States have a functional definition (i.e. definition which is used for day-to-day policing, most often described as information collected during the performance of their tasks).
3) 13 Member States have a legal definition of the term 'police record' (some Member States have a legal as well as a functional definition). However, in most cases the content of the definition is of general nature, without specifying the type of information, authorities, categories of persons or types of offences on which such information can be collected or processed.

Subsequently, having a detailed definition of the 'police record' at EU level was not the favoured option by the consulted Member States. Even though a few countries pointed to several elements for including them in the common definition, if it existed, such as categories of persons or types of information, all respondents supported the definition in its broad form. Whereas it seemed impossible to achieve consensus if constituent parts were to be specified, Member States were unanimous in supporting the inclusion of the purpose of criminal investigations in the definition.

Based on the above observations, the study team has developed the following suggestion for definition for a common terminology of a "police record" at EU level:

A 'Police Record' shall mean any information available in the national register or registers recording data of competent authorities, for the prevention, detection, investigation and prosecution of criminal offences.

The very broad nature of the proposed definition implies that, if accepted by Member States, its use could be further extended not limiting it to EPRIS context. Since the main focus lays in the purpose or finality for which the records would be used, the definition could be equally applied by other law enforcement authorities performing their tasks for the same pre-defined purpose. The finality principle has been recognised in other EU instruments such as the Prüm Decision (which is directed to 'authorities responsible for the prevention and investigation of criminal offences'[21]) or the Swedish Framework Decision (which is geared towards 'competent law enforcement or judicial authorities, including public prosecutors, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts'[22]). At the same time, it might be worth considering the possibility of employing the term 'criminal investigation records', instead of 'police records' to better reflect the *rationale* of the approach chosen. As a consequence, as a long-run perspective, the name 'European Criminal Investigation Records Index System (ECIRIS)' could be used to replace the current title for the European Police Records Index System (EPRIS).

The suggested broad definition reflects a common view of Member States on what they consider to be a 'Police record' in its wide sense. This does not presuppose however that certain limitations are not possible regarding the authorities involved, the categories of persons concerned or the related offence types. These limitations are further detailed in the description of the EPRIS system design. It is advisable that they would also be specified in the legal instrument governing EPRIS. The same could be said about other EU initiatives should the 'criminal investigation records' definition in future be used for their purposes.

5.4 Evaluating criminal justice cooperation

The European Commission, in cooperation with Europol should monitor and evaluate the effectiveness and efficiency of EU cooperation and information exchange with criminal justice finality.

This will lead to a better understanding of:

- the actual willingness and capacity to make use of the Europol Information System;
- the potential of additional functionalities that may be used to increase the value of existing systems;
- the need for, and benefits of a new, specific EPRIS system.

The following components should be monitored:

- Number of unsuccessful international police record requests to other EU Member States (to measure the opportunity costs of not implementing an automated search system);

[21] Art. 1 Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Decision), OJ L 210 6.8.2008, 1-11.

[22] Art. 2(b) 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 (Swedish Framework Decision), OJ L 386 29.12.2006, 89-100.

- Costs (in particular, time and resources) related to international police record requests to other EU Member States;
- Users of EIS;
- National databases used to feed the EIS;
- Number of person records in the EIS that can be used for hit/no-hit searches;
- Number of EU-wide police record requests related to crimes outside of the Europol mandate;
- Use of SIENA;
- Number and type of automated processes supporting the international exchange of police records;
- Data quality of police records at national level and exchanged records at EU-level.

By January 2015, the EIS should have a more extensive user base (e.g. 10 000 users), show a substantial increase in the amount of active users (using the system directly or indirectly) and contain more than 200 000 person records (for hit/ no-hit queries). Otherwise it is unlikely that it has a real chance of becoming a credible instrument that can allow law enforcement officers to determine whether police records exists in another EU Member State.

If the evaluation was to find that there is a need for a new system, a pilot project can be started based on the EPRIS system design outlined in *Section 5.5.1* A Pilot Project can be set up between a limited number of Member States (with a high potential for cost reductions and a high amount of international transactions). Such a project can lead to a more informed evaluation of the technical feasibility and impact of a new, specific EU-wide EPRIS system. It is therefore highly recommended to consider international and EU standards at the onset and involve EU institutions and relevant agencies as observer. If the pilot project is considered a success then the project could be developed as an EU wide system. This would imply initiating a legislative proposal at EU-level and the development and implementation of an EPRIS system based on concrete lessons learned.

5.5 EPRIS design

The current research has provided valuable information related to system specifications that seem adequate if a new, complementary EPRIS system were to be set up. This section describes the findings and suggestions in more detail.

Indeed, there might not be a need to develop such a system at EU-level if existing systems and on-going EU projects are used and further developed to their full potential. However, there are sufficient indications that the business needs expressed in the course of this study might still remain largely unaddressed in the coming years. If that proves to be the case, setting up a specific new EPRIS system at EU-level will be necessary.

A number of Member States might be tempted to initiate an inter-governmental pilot project based on the following architecture as soon as possible to test its viability and address existing needs. This can lead to useful lessons learned and may prove to be the foundation for further EU progress in this domain. After all, intergovernmental pilot projects have also been at the basis of Prüm or EU criminal records exchange. But this approach carries the risks of scalability of technical solution as well as EU divergence and inconsistencies in the domain of police cooperation. To mitigate that risk and ensure a constructive outcome of any pilot project it is strongly advised that any such initiative be combined with the following engagements:

- Strong and unwavering engagement towards full implementation of existing systems and on-going EU projects.
- Full integration of existing EU standards (UMF2, EULOCS).
- Full transparency towards other EU Member States and relevant EU institutions with respect to information exchange statistics, costs and benefits.
- A strong cooperation with Europol to ensure complementarity and possible integration with its systems.

5.5.1 System architecture

The preferred and recommended system architecture should have a semi-centralised character that incorporates the following elements:

- No information should be stored centrally, at EU level:

  18 Member States have expressed their preference for this approach. This is in accordance to the subsidiarity principle in this context, allowing the principal data owner, the Member State authority to retain control over the information directly and manage the creation, editing, updating and deletion of data.

- The EPRIS query system could be triggered automatically by a query in a national system or after query selection by the users:

  This is in accordance to the subsidiarity principle in this context, allowing the principal data owner, the Member State authority to retain control over the information directly and manage the creation, editing, updating and deletion of data.

- A central forwarding system at EU level could relay queries from requesting countries to receiving countries:

  14 Member States have expressed their preference for this approach. This enables a consolidation of the requests at central level, the use of a common reference format that can be tested in an efficient manner and limits the initial communication to one query signal from the investigating Member State.

  The reference architecture would not impose limitations on how the systems would be interconnected. Either systems would be interconnected through a forwarding system, or they could be connected in a point to point manner. Creating a new communication system is an option, but re-use of existing systems would be much more cost effective. Given the current state of play the preferred communication network would be Europol's SIENA. This system offers communication between all Member States through the national Europol National Unit. This would mean that there is no need to set up another secure communications networks or spend time setting up a forwarding system. Currently the development of automated system-to-system communication is still in testing phase. However, as soon as it is live, this would make SIENA the ideal candidate for message exchange because it offers the most comprehensive and complete access to Member States and is specifically designed to be an extensible message exchange platform.

- Information from a limited number of data fields from existing national law enforcement databases should be extracted and converted to a standard EU format into an EPRIS national database managed and controlled at Member States level.

  The use of national extracted copies is recommended because of the following reasons:

  - *Performance*: The local MS database (DB) would probably not sustain a high number of requests coming from the other MS. The sizing of the number of requests that the local MS DB can sustain is done by design and estimated on the number of local requests.
  - *Security*: It is not recommended to give direct access to a local MS DB from a system which is not under control of the local MS. The risk to give potential access to the entire local MS DB is higher than just giving access to an extracted DB including only the necessary information. Giving direct access to the local MS DB is against the security principle of defence in depth.
  - *Flexibility*: In case of future improvements of the EPRIS functionalities and data model, it will be easier to make the changes on an extracted DB in order to limit the impact on the national DB operations.
  - *Reusability*: The extracted DB and the information exchange software could be created once and be reused by multiple (or all) Member States.

- Queries launched from one Member State should be executed in all EPRIS national databases. The responses would be hit/no-hit responses with additional information:

  As there is no certainty about which EU Member State might have information it is recommended that the query is executed automatically in all EU Member States when a search in EPRIS is initiated.

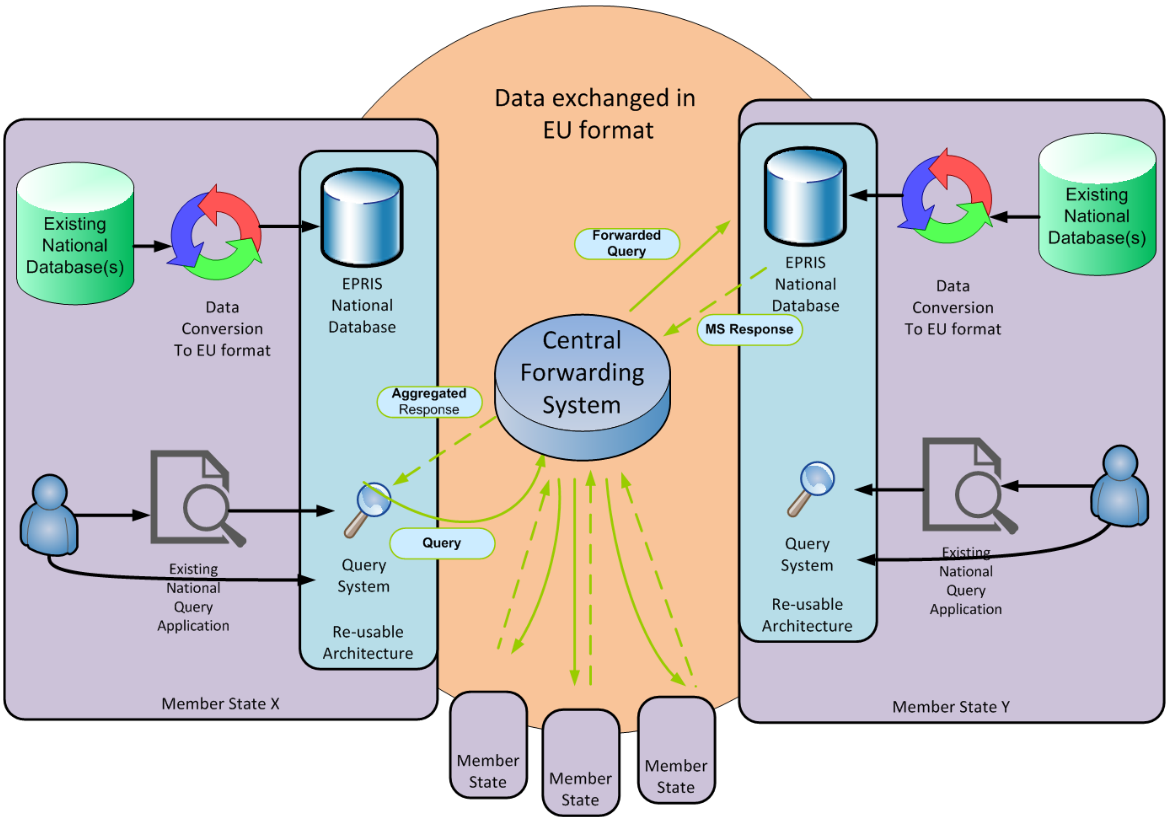
- The consolidated query response should provide a list of “hits”, enlisting Member States where information on the queried individual is available together with contact data of the national contact point and categorised information concerning the offence type for which an individual has been suspected and the date of offence. The system would also enlist Member States for which there was no response to the query or produces a general, consolidated response that “no information was found” for all EU Member States:

  18 Member States have expressed their preference for this approach. Response clarity supports efficient decision making as to whether or not further bilateral communication is necessary and urgent.

- Bilateral information exchange accompanied by a clear statement of the purpose of the information request takes place between the national contact points:

  Intervention by national contact points allows for a validation of the decision to transfer information and decreases the likelihood of false interpretations.

The following image depicts the recommended technical architecture[23]:



Data exchanged in EU format
Existing National Database(s)
Data Conversion To EU format
EPRIS National Database
Aggregated Response
Existing National Query Application
Query System
Query
Re-usable Architecture
Member State X
Forwarded Query
Central Forwarding System
MS Response
EPRIS National Database
Data Conversion To EU format
Existing National Database(s)
Query System
Re-usable Architecture
Existing National Query Application
Member State Y
Member State
Member State
Member State

Figure 6: Recommended technical architecture

The recommended technical architecture is based on a decentralised data storage architecture, where each Member State would remain responsible and in control of its police information. It is designed in a modular manner to be able to keep the different required operations separate. This permits standardisation, promotes re-use and simplifies development work. Information would be retrieved from the existing national database (represented in green in the diagram above) in an EPRIS national database. This would only contain the necessary information required for the system to permit searches and return a hit or no-hit answer together with offence type/date data and contact information identifying the contact partner for the bilateral communication phase. The data would be converted into a standardised EPRIS format (currently referred to as the EU format). This conversion step would ensure that the extract database model is the same across Member States. This would facilitate upgrading operations and would permit the re-use of one single query software. The data conversion step would be MS specific as it would depend on how the data is stored in the Member State database. So this step would require customised development for each Member State.

After conversion, the data would be stored in the EPRIS national database and it is only the data in this database against that queries from other Member States would be run. This means that the current national database would only be experiencing more load from the periodic data extraction but it would not have to handle the load of all Member State queries. A second advantage is the increased security this option offers as only a subset of the data would be 'searchable' (not browseable) from the other Member States.

[23] The suggested solution is also valid for a point to point communication model.

As the data is in a standardised format, there would be only a need to develop a query component once. This could be implemented as a stand-alone solution, but preferable as a service that could be integrated into the Member States existing national query application or in other querying tools (for example the European Information Exchange Platform (IXP) when it is available).

5.5.2 Data and formats

Identification data should deliver sufficient certainty to be able to unequivocally match a record with a query originating from an investigating Member State.

The following data fields should be included in the national data copy:

Identification data category	*Modality*
First name; Surname; Date of birth; Gender;	Mandatory
Aliases	Included as first name (and last name)
Nationality	Foresee as optional field - According to Manual of Procedure
Photo (to allow for future facial recognition)	Foresee as optional field - According to Manual of Procedure
National identification number	Foresee as optional field - According to Manual of Procedure
Father's name / Mother's name	Foresee as optional field - According to Manual of Procedure
Any other identification data: e.g. Residence or known address; Surname at birth; Scars/marks/tattoos; Place of birth (town and State); …	Excluded: (In national or local file)
Fingerprints/DNA/VRD	Excluded: via Prüm

Table 16: Recommended data fields

It is considered essential for some Member States to have a system which facilitates the provision of information in addition to a hit. The pure hit/no-hit process would not be sufficient in light of the existing workload. For this reason, the following data is added.

Data category	*Modality*
Type of offence	Mandatory, if available in the national databases; using the EULOCS offence classification
Date of offence	Mandatory, if available in the national databases
Country of data entry	MS to be contacted for further information
Criminal Record Information	Excluded: via ECRIS
Any other object/event identifiers	Excluded: via EIS or other exchange mechanisms

Table 17: Recommended additional data fields

The responses to the study questionnaire and feedback received during the country visits revealed that slightly more than a half of Member States (16 out of 27) supports the suggestion to limit the information exchanged via EPRIS to certain, and not all offence types. Most Member States refer to the European Arrest Warrant offences as a point of reference (6 Member States), crimes falling under the Europol mandate (2 Member States) or the ECRIS list (1 Member State). Also, several Member States stated searches through EPRIS should concern offences which are punishable by imprisonment in the requesting state (the time ranging from one day to one year, depending on the respondent).

Among the arguments which might have impacted the choice of 11 Member States to opt for the 'all offences' approach could have been the possible added value of EPRIS for national criminal policy. A broad scope of crimes implies that the tool would be used also for offences often committed in Member States but not considered as priority in the context of international cooperation and thus not listed in respective EU legislation. Additionally, a decision to extend EPRIS to all criminal offences could be well justified by the Swedish initiative rationale, which stipulates that 'Member States shall ensure that conditions not stricter than those applicable at national level for providing and requesting information and intelligence are applied for providing information and intelligence to competent law enforcement authorities of other Member States'.

However, the principle of availability should be well balanced against proportionality and necessity criteria. The decision on whether the system will be based on hit/no-hit responses or additional information will be provided apart from the hit other well established EU law principles are thus important in this context. Since the majority of respondents reported that they see the need in more information communicated in addition to a hit, it is advisable to first enable the Member States to link their information on certain categories of offences. Once this functionality is tested in practice and assessed positively, the opening up of the tool for all offence types could take place.

Data update can take place on a daily basis. Data deletion takes place according to national rules of deletion. If data is deleted from the national criminal investigation records, it must be deleted from the national extract in the following up-date.

All relevant criminal investigation records from police authorities would have to be uploaded with the exception of data excluded for reasons of national security. Data from other competent authorities working with criminal justice finality may also be uploaded to the national EPRIS database. Criminal Record Authorities could also be requested to upload some data to the national EPRIS database.

5.5.3 Categories of persons

Throughout the EU, information in police records relates to different categories of persons. Whereas all Member States have reported that they record information on the offenders or suspected offenders, this is less often the case for other categories, such as victims.

According to Member States' responses, queries in future EPRIS should be limited to certain categories of persons: suspected persons and perpetrators. After all, the large majority of respondents do not see the need to make searches on victims and witnesses.

It is thus recommended that in the short run, suspected persons should be at the core of the information exchange through EPRIS while setting a legal obligation to exclude victims, associates and witnesses from the list of categories of persons concerned. Also, no automatic data uploading should be allowed unless it is confirmed that the information extracted from the police records national database does not fall within one of the three mentioned categories. According to the international practice and in compliance to established data protection principles, only persons who have been considered as suspects for the last 3 years, could be targeted for investigation checks through EPRIS. Furthermore, the system should foresee the long-term possibility to make searches also on convicted persons (connecting EPRIS with ECRIS). Since only in a few Member States police records systems are interconnected with the courts case management systems, this is not included in the short-term vision of an EPRIS system.

5.5.4 Access and searching modalities

Majority user requirements	***Recommendation***
Manual searching	Needed and recommended
Searching based on combined criteria	Needed and recommended Should allow for full flexibility for the users - no mandatory search fields
Automated cross-checks	Is considered useful by user community but relatively complex from a technical and legal perspective and sensitive from a political perspective. Not recommended for initial phase.

Table 18: Searching modalities

During the consultation round, the majority of Member States agreed that multiple authorities performing criminal investigation tasks could have access to EPRIS. These include police, border guard, custom, inspection and prosecution authorities as long as they perform actions with criminal justice finality. The lower number of Member States in favour of granting access rights to inspection services could be explained by the fact that there is little coherence in this field: in some countries inspection services are part of the police services, whereas in others they carry out administrative rather than criminal investigations.

Several countries noted however that in their countries, existing legal obstacles do not allow different law enforcement authorities to access the police records system. A concern has been expressed about providing access to different governmental agencies from other Member States whereas comparable local governmental agencies do not receive this access. In one Member State, a clear objection to broadening the scope to all law enforcement authorities was expressed arguing that EPRIS should first focus on the police related data and when the system is tested and its efficiency is proven, the extension of its scope should be considered.

Considering the above, the study team thus suggests focusing on police authorities as a mid-term perspective with the possibility to extent the access to EPRIS to other law enforcement performing criminal investigation tasks authorities in the long-run. Taking into account that the issue of interconnection between different national competent authorities has been reported by a number of Member States and reforms to change the situation are foreseen to be completed in only some of them, it is indeed advisable to exchange data between police authorities in the narrow sense with the possibility to involve other relevant competent authorities in future.

To sum up, on the basis of stakeholder feedback presented in the user needs section we recommend that:

- Police authorities have direct access to the system from the onset;
- Other competent authorities working with a criminal justice finality have indirect access to the system (via the criminal investigation liaison authority) - they may obtain direct access at a later stage;
- Europol has direct access to the system, other EU agencies may apply.

At a later stage, access could be arranged via the European information exchange platform (IXP) when that project has been implemented.

5.5.5 Management Structure

The organisation of the information flow entails three phases that require management and support:

- Information request;
- Information processing;
- Information provision.

Even though, three phases could be performed by one authority or by several distinct authorities working together in the Member States. We recommend that one central authority performs these three functions in each Member State to keep coordination costs to a minimum. Central points of contact can act as main liaison units in the law enforcement related information exchange. They must work closely together with local units at national level and should be responsible for storing the necessary information in the respective national database and providing answers to requests in the form of bilateral exchanges.

Institutions and bodies at EU level would exercise a rather limited role. But if a specific new EPRIS system is set up there will be a need for an organisation or department ***at EU-level*** that:

- Ensures the availability and security of the network infrastructure;
- Coordinates (further) development and maintenance of a central technical component (if applicable);
- Assists Member States’ authorities with integration and interfacing challenges;
- Provides technical capacity support to Member States;
- Oversees general data flow statistics and supports data protection auditing.

The team in charge of the operations at EU level will design, develop and maintain the central component of this option, the forwarding system. It should also guarantee a high level of service availability and provide assistance to new countries joining the network. This institution would have an operational support role. It would also act as an auditor and would ensure the provision of reliable statistics.

The agency for large scale IT systems could manage the system. In the case of a pilot project between Member States, one Member State could assume responsibility for managing the central forwarding system. In the latter case, also the agency for large scale IT systems should be involved. Two informal working groups, consisting of technical and legal experts could be established. They would meet on a regular and ad hoc basis before and after the system becomes operational. The technical working group would determine the technical specifications whereas the legal working group would oversee the legal developments. In this way, it would be possible to introduce technical improvements and legal expertise and guidelines gradually. Once the system becomes operational, the EPRIS working groups could become an end-user forum where project members report on their experiences.

Alternatively if SIENA is re-used, some of the tasks listed above can be carried out by Europol as they are already managing the operations of the SIENA system. They are coordinating its further development and assisting and supporting Member States. According to Article 10(1) of the Europol Decision, Europol has the right to maintain other systems processing personal data, which in this case could be an EPRIS system with an integrated SIENA tool. Depending on the level of customisation that is possible on the SIENA system and the specific needs that are required it can be left up either to Europol or the agency for large scale IT systems to oversee data flow statistics and data protection auditing.

Another option to simplify and cut cost would be to have the EPRIS national databases (the extract from the national police database) operated and maintained by Europol and hosted at the ENU of every Member State. This would imply that the database and query system can make use of the same software in all Member States, which would mean a substantial cost saving as it would only have to be developed once. The system could also be operated, maintained or supported centrally which would also lead to substantial savings on operational expenditures for Member States.

At national level, an EU network of Member States' Criminal Investigation Liaison Authority should be set up, responsible for (in cooperation with local units):

- Channelling requests for information from local law enforcement units when they are not able to do a query directly in EPRIS;
- Channelling requests for information from law authorities who only have indirect access to the system;
- Supporting requests for further information in bilateral exchanges;
- Supporting the provision of answers to requests in bilateral exchanges;
- Ensuring data upload (if applicable);
- Ensuring responses to information queries (if applicable).

The report on Police Cooperation adopted by the Council of the European Union[24] in 2005 recommended that Member States should adhere to the "one-stop-shop" principle for better coordination and facilitation of work carried out by law enforcement authorities. Following this approach, in some Member States, different contact points, such as the SIRENE Bureau, the Europol National Unit (ENU), the Interpol National Central Bureau (NCB) and the office responsible for the liaison officers' network, have been integrated into one office. Guidelines and good practices for the establishment and organisation of such integrated offices are set out in the Manual of Good Practices concerning the

[24] Report from the Police Cooperation Working Party (Mixed Committee EU/Iceland, Norway and Switzerland, Liechtenstein), 10505/4/09 (REV4), 14.12.2009

International Police Cooperation Units at National Level[25]. The creation of central authorities/integrated offices does not necessarily imply that all related activities fall under their competences however. On the contrary, in accordance with the principle of subsidiary, relevant tasks should be carried out at the level where they can be best dealt with. Direct contact undertaken between local law enforcement authorities or experts is another possibility for cooperation between relevant authorities.

Local law enforcement units also play a role in aforementioned three phases of the information exchange mainly to ensure proper information entry and query procedures.

Several interviewees have stressed the importance of efficient follow-up mechanisms and efficient bilateral information exchange mechanisms. This depends both on the level of automation as well the capacity of the authorities involved either at central, national or local level.

National data protection authorities should be responsible for monitoring whether the creation of a national copy with data complies with the data protection requirements and for handling claims regarding misuse/abuse of the system. Further discussions may be needed (possibly at the level of Article 29 Working Party on Data Protection[26]) as this concerns the coordination of work carried out by national data protection units. A central support structure (e.g. the European Data Protection Supervisor) can be involved to ensure the coordination of data protection supervision.

5.5.6 Legal framework

If the proposed semi-centralised system is opted for, there will be no need to set a legal obligation to store data as no information will be stored centrally. A forwarding system would only relay queries from requesting countries to receiving countries. However, in order to have an efficient information exchange system, legislation would be necessary for data upload in national extraction databases. New legal provisions would probably have to govern automated data processing via EPRIS. Similar to the provisions of Article 3 of Framework Decision 2009/315/JHA[27], an article governing the information exchange through one point of contact per Member State for the purpose of EPRIS could be included in the new legal instrument. The Swedish Framework Decision could serve as an adequate legal basis for receiving additional information requested following a positive hit. It would thus cover only the second stage of the information exchange via EPRIS.

5.5.6.1 Data protection safeguards

In order to comply with the established data protection principles, the following elements should be taken into account:

- *Purpose limitation*: it is suggested that the new tool for the police records information exchange would be used in the context of criminal investigations and

[25] Manual of Good Practices concerning the International Police Cooperation Units at National Level, 7968/08 ENFOPOL 63+ COR 1 and 2

[26] Available from: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

[27]Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93/23 of 07.04.2009.

would not concern administrative policing. In this way, the core objective of preventing and combating crime within the EU can be targeted.

- *Proportionality:* it is of the utmost importance that processes facilitated via EPRIS constitute only a minimal interference necessary with regard to the legitimate aim. In this respect, the following policy options are preferred:

  - The system should function on hit/no-hit basis (with the possibility to provide a minimum necessary amount of additional data fields (e.g. type and date of offence);
  - Search should be conducted in 27 national extraction databases containing identical data fields with information necessary for identification;
  - No biometric identifiers should be used, the option of photographic material can be considered.
  - There should be an ability to refine the queries, using multiple search criteria, thus limiting the hit/no-hit results and avoiding the sharing of irrelevant information and false positives.
  - Searches within EPRIS should be limited to competent authorities in criminal investigations.

- *Subsidiarity*: According to the principle of subsidiarity (Article 5(3) of the Treaty on European Union (TEU))[28], action at the European Union level shall be taken only if, and in so far as the objectives envisaged cannot be achieved sufficiently by Member States, but can rather, by reason of the scale or effects of the proposed action, be better achieved by the Union. In the light of the problems outlined above, the analysis of subsidiarity indicates the necessity of EU-level action on the following grounds:

  - The pre-study on EPRIS revealed that 13 on 16 respondents think the exchange of police records should be improved at the EU level.
  - The development of EPRIS will benefit from existing EU facilities, such as SIENA or the possible management by the EU agency for large-scale IT systems.

- *Effective control on data*: following aspects should be monitored in order to ensure the effective control of the data exchange:

  - *Data access*: only authorised competent authorities should get access to EPRIS. To ensure efficient control, Member States should hand over a list of designated authorities and their purpose to the European Commission, which should then publish the list in the EU's Official Journal to maximise transparency and accountability. No intelligence agencies should access EPRIS, not even when they work with criminal justice finality. Data access also implies the possibility for a data subject to request rectification or erasure of personal data.
  - *Security measures*: apart from general provisions on the security of data processing set in Article 22 of the Council Framework Decision on the

[28] Treaty on European Union (Maastricht treaty), OJ C 191, 29.07.1992.

protection of personal data processed in the framework of police and judicial cooperation in criminal matters, various security prerequisites are used across EU Member States, the most common being confidentiality, integrity, availability non-repudiation and authenticity.

  - *Supervision*: another important prerequisite of the data exchange mechanism within the future EPRIS is the supervision system. In the semi-centralised system scenario, a model involving a supervisory authority both at the national and EU level might be a suitable solution.

- *Monitoring and evaluation*: The establishment of the EPRIS necessitates the setting up of an adequate monitoring mechanism. This would include gathering relevant statistics in order to monitor the fulfilment of operational objectives of the EPRIS. Regular experts meetings should be organised to enhance the effects of a coherent and efficient system implementation. Finally, a regular evaluation can also ensure an adequate supervision of the respect for data protection guarantees. For this purpose, statistics may include elements such as the number of requests for access or rectification of personal data, the length of the update process and cases of security breaches. Such data and the relevant reports should be made fully available to national data protection authorities.

5.5.6.2 Applicable law and procedure

With the adoption of the Lisbon Treaty and the abolishment of the three pillar system, matters related to judicial and police cooperation in the European Union have become subject to the co-decision procedure, also called an 'ordinary legislative procedure' and described in detail in Article 294 of the Treaty on the Functioning of the European Union (TFEU). Co-decision procedure will thus also apply to the possible establishment for EPRIS constituting a measure "concerning […] collection, storage, processing, analysis and exchange of relevant inf*ormation"* (Article 87 of the TFEU**)**. Similar to formerly existing Framework Decision which was extensively used in the field of judicial and police cooperation, a new European Union legal act – directive – will be governing the instrument, if a decision to establish EPRIS would be taken. Adopted by the Council of the European Unison in conjunction with the European Parliament on a proposal by the European Commission, a *"directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods"* (Article 288 of the TFEU). The main purpose of a directive is to align national legislation.

5.5.7 Impact

Estimating the impact and costs and benefits of setting up a new, specific EPRIS system at this stage is very challenging as there is a wide range of determining factors and insufficient statistical information available. The costs also depend on the future use of, and integration with existing systems. This section should therefore be read with caution; it merely aims to provide a general indication of the costs and benefits serving as a starting point for later reference.

The following table presents one-time average development and recurring investments estimates, both at EU-level and at Member State level:

One-time development investment		
EU Central Site		***Member State***
Item	***Price (K EUR)***	***Price (K EUR)***
Design	300	100
Hardware and licenses	150	50
Software development	600	250
Installation	100	20
Testing	250	100
Project management	200	80
Lab	40	10
Communication setup	20	10
Crypto devices	50	10
Documentation and procedures	50	20
Monitoring	20	10
Total (one-time)	**1780**	**660**
Recurring investments per year/per site		
EU Central Site		**Member State**
Item	**Price (K EUR)**	**Price (K EUR)**
Communication	10	5
Solution maintenance and support	100	120
Operations (24x7)	1200	1000
Management	150	80
Total per year	**1460**	**1205**

Table 19: One-time development and recurring investment estimates

The cost evaluation is based on similar exercises done in the frame of EU studies, such as CIWIN, HEOF or EUROSUR, and on the cost estimation provided by one Member State for a semi-decentralised solution. It includes fixed costs for the set up and the implementation of the solution and yearly recurring costs. The fixed costs include the design, the purchase of the hardware, the development of the software, the implementation and the effort to write the documentation and procedures. The recurring costs include the yearly subscriptions, maintenance and support of the different software and hardware components and the human effort to operate the solution and to support and maintain it up-to-date. The estimation is conducted for an unclassified system and does not therefore include the effort needed regarding the accreditation of the solution to a certain level of classification.

It should be noted that fixed development costs in the Member States may be higher depending on the number of information systems involved. For example, if there are several police authorities in a certain country managing different information systems, national costs may be higher. But in that case, this project could also help that Member State to further integration at the national level. This table does not take inflation into account for recurring investments but this is more than compensated by the fact that maintenance costs are likely to decrease over time because of productivity improvements. Substantial cost reductions may be possible at Member State level due to comparable solutions in place, previous arrangements with service providers and lessons learned from other EU projects.

Total investment needs estimates with potential additional risks caused by a new system are presented below:

Total costs EU (27 Member States)	
Fixed one-time development investment	
Item	***Price (K EUR)***
Fixed development costs central site	1780
Fixed development costs Member State site	17 820 (=660x27)
EU Total	**19 600**
Recurring investments (K EUR/year)	
EU central site recurring costs	1460
Total yearly MS sites recurring costs	32 535 (=1205x27)
EU Total[29]	**33 995**
Additional recurring risks/costs (not quantified)	
Damage caused by erroneous (non-) actions based on information of insufficient quality (e.g. false hit information or false no-hit information)	
Damage caused by erroneous (non-) actions based on information overload	
Damage caused by complacency created at national level by over-reliance on information gathering by other law enforcement authorities in EU	
Increased probability of occurrences of police information leakage to non-competent authorities or third parties – damage caused by related unwarranted privacy breaches	

Table 20: Total investment needs

The benefits are harder to quantify at this stage but may be very substantial and far outweigh the costs. The following table presents an overview of the possible positive impact of a well-functioning EPRIS system. A pilot project and a complementary detailed evaluation study could provide further clarity on the exact scope of both costs and benefits.

Non-quantified benefits EU (27 Member States)
Related to signalling of high risk individuals
Decrease number of injuries or deaths of law enforcement officers and damage to law enforcement officers tools (e.g. police cars)
Related to efficiency of investigative work
Decrease in the number of non-necessary international requests[30]
Shortened duration of some investigations
Shortened duration of EU information exchange transactions
Reduction of the number of full time equivalent investigators needed/completed investigation (e.g. by decreasing the duplication of efforts (e.g. in cases where there are on-going investigations on the same person throughout the EU))
Improved national data quality based on an increase in bilateral information request responses
Improved coordination and support by EU law enforcement agencies having query access to EPRIS

[29] It should be noted that these estimates do not take inflation into account.

[30] To illustrate this point: authorities of a Member State currently send approximately 100 000 international requests per year. But because they do not know who to address the request to, only 40% of these requests lead to a response. This points to substantial cost cutting potential in relation to the preparation of international requests and responding to unnecessary requests.

Related to effectiveness of investigative work
Increased speed at which crimes are detected
Decreased number of unnecessary pre-trial detention days
Decreased number of unnecessary court proceedings
Shortened court proceedings because of availability of additional proof
Decreased sense of impunity of internationally active offenders
Decreased crime rate and decreased society cost of crime
Other
Improved citizens’ trust in EU law enforcement system/coordination
Improved citizens’ sense of security

Table 21: Non-quantified benefits

6 Annexes

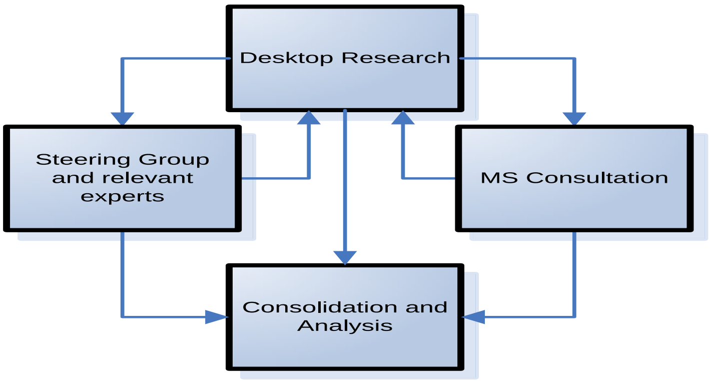
Annex 1: Acronyms and Abbreviations

Acronym Abbreviation	***Meaning***
AFIS	Automated Fingerprint Identification System
ANSI/NIST	American National Standard for Information Systems/ National Institute of Standards and Technology
CIS	Customs Information System
DG HOME	Directorate General Home Affairs
DNA	Deoxyribonucleic Acid
EC	European Commission
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms (also called “European Convention on Human Rights”)
EDPS	European Data Protection Supervisor
ECRIS	European Criminal Records Information System
EIS	Europol Information system
ENU	Europol National Unit
EPRIS	European Police Record Index System
EU	European Union
EULOCS	EU Level Offence Classification System
EUROPOL	EU agency supporting and coordinating the cross-border criminal investigations within the EU.
EC	European Commission
FIDE	Customs File Identification Database
GSC	General Secretariat of the Council
IRCP	Institute for International Research on Criminal Policy
IG	Interview Guide
IXP	Information Exchange Platform
MS	Member State
PR	Police Record
PRÜM	Framework provided by the Prüm Decision allowing for the automated exchange of DNA, fingerprints and vehicle registration data between 27 EU Member States
QST	Questionnaire
SIENA	Secure Information Exchange Network Application
SIS II	Schengen Information System II
SPOC	Single Point of Contact
s-TESTA	Secure Trans European Services for Telematics between Administrations
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UIS	Unisys
UMF2	Universal Message Format 2
VRD	Vehicle Registration Data

Annex 2: Methodology

This section describes the approach followed by the study team when conducting the present feasibility study. As shown in the figure below, it consisted of four main building components:

- Desktop research;
- Guidance from members of a Steering Group and other relevant experts;
- Consultation through questionnaires and visits to Member States;
- Consolidation and analysis.


Desktop Research
Steering Group and relevant experts
MS Consultation
Consolidation and Analysis

Component 1 – Desktop Research

Desktop research mainly consisted of studying relevant documentation and internet research. It represented the basic methodological step for determining the relevant normative and institutional framework and identifying conducted studies and available reports. The desktop research was useful both to obtain an initial knowledge base and to complete the information obtained during the Member States visits and Steering Group meetings. Desktop research was an essential part of any assessment since it allowed interviews and meetings to take place in a more focused manner and thus formed the basis for interaction with national contacts.

Component 2 – Guidance from the Steering Group and other relevant experts

As part of the study methodology, the Steering Group consisting of experts from the European Commission representing main study fields provided relevant information to the study team and facilitated the communication with the relevant experts. These included specialists representing other large scale information systems relevant in the context of EPRIS, such as Prüm, ECRIS or Customs files identification database (FIDE), as well as the European Data Protection Supervisor (EDPS). Several visits to Europol were conducted where existing systems and tools as well as new initiatives in the field of cross-border information exchange were presented to the study team.

Component 3 – Member States consultation

In order to ensure that the proposed solution takes into account the concerns and suggestions of the Member States, the consultation process was launched in the beginning of the study taking form of the study questionnaire (sent to all Member States), interview guide (sent to those Member State to which the study visits had been scheduled), study visits themselves (scheduled to twelve Member States) and communication with the representatives from Member States authorities conducted via e-mail or telephone.

The target groups in the Member States were law enforcement authorities dealing with criminal investigations (e.g. police, inspection services, customs, etc.) as well as other relevant authorities, such as authorities managing the national AFIS or national data protection authorities. The cooperation with the different experts representing the above mentioned authorities took place through the nominated Single Points of Contact (SPOC) who coordinated the work at national level for the purpose of the study.

Additionally, the Expert meeting that was organised in Brussels in the course of the study constituted an opportunity to gather and consult at once a wide range of experts and practitioners.

Component 4 – Consolidation and Analysis

Once the information was collected through desktop research and by means of answers to the study questionnaire and interviews in the Member States, the analysis of the information was conducted. It included legal, business and ICT assessment and consisted of two main steps: the evaluation of the current situation regarding the police record related information storage and exchange at national level and Member States' views on the proposed scenarios for the EPRIS. The results were assessed in the light of relevant studies, policies, legislation and case law. The intermediary findings presented in the interim report were further elaborated once all study visits to Member States and meetings with relevant experts at EU level were conducted. The study final report (the present document) comprises the key information collected in the course of the study and the study team's recommendation on the preferred solution.

Annex 3: List of contacts undertaken at national and EU level

National level: Single Points of Contact

MS	*Organisation*
AT	Federal Ministry of Interior
BE	Belgian Federal Police
BG	Documental funds and Inquiry Activity Unit, Inquiry Activity, Communication and Information Systems Department within Chief Directorate Criminal Police, Ministry of Interior
CY	Cyprus Police
CZ	International Relations Division, Police Presidium of the Czech Republic
DE	German Federal Criminal Police Office
DK	National Communications Centre
EE	Central Criminal Police, Police and Border Guard Board
EL	Forensic Science Division, Hellenic Police
ES	Unidad de Documentación de Españoles y Archivo. Cuerpo Nacional de Policía
FI	Police Department, Ministry of the Interior
FR	Division of the International Relations, Central Directorate of the Judicial Police
HU	Ministry of Interior
IE	An Garda Síochána
IT	International Police Cooperation Service
LT	Ministry of Interior
LU	Service de Police Judiciare (SPJ)
LV	Information Centre of the Ministry of the Interior
MT	Malta Police Force
NL	Ministry of Security and Justice in the Netherlands
PL	International Police Cooperation Bureau, National Police HQs
PT	International Cooperation Unit – Criminal Police
RO	Ministry of Administration and Interior
SE	National Police Board
SI	IT and Telecommunications Office, MOI Police
SK	Europol National Unit
UK	Home Office

EU level: Steering Group members

Organisation
European Commission, DG Home/Unit A3
European Commission, DG Home/Unit C2
European Commission, DG Justice/Unit C3

EU level: Experts on large scale IT systems

Organisation
Europol
DAPIX Prüm subgroup on fingerprints data
European Anti-Fraud Office (OLAF)

Annex 4: List of organisations interviewed

Organisations consulted during missions to Member States

MS	*Organisation*	*Date*
BE	Federal Police CGO	17/01/2012
CZ	SIRENE Bureau CZ	06/02/2012
	Concept and Informatics Development Division, Police Presidium	
	International Relations Division, Police Presidium	
	General Directorate of Customs, Police Presidium	
	Personal Data Administration and Control Section, Police Presidium	
UK	Home Office	09/02/2012
DE	Division Information Technology, Product Management, Bundeskriminalamt	23/02/2012
	Division Central CID Services, Police Information & Data Services, Bundeskriminalamt	
	Division Central CID Services, Staff, Bundeskriminalamt	
PL	National Police HQ's EPRIS	28/02/2012
	Forensics of the National Police HQs	
	IT Bureau of the national Police HQs	
	Criminal Intelligence Bureau of the National Police HQs	
	Border Guard HQs	
	Customs Service, Ministry of Finanse	
	Legal Bureau of the National Police HQs	
BG	IOCD	05/03/2012
	RIFSC	
NL	Ministerie van Veiligheid en Justitie, international police cooperation matters	08/03/2012
	National Police Agency	
	ICT police	
	Regional Police Force The Hague	
FI	Ministry of the Interior	12/03/2012
	NBI	
	ICT Agency	
ES	C.G.E.F.	16/03/2012
	SGSICS	
	SIRENE GRUPO DAPIX	
	CNP	
	CNP-INFORMÁTICA	
	CNP-ARCHIVO CENTRAL	
	CGPJ-UCIC	
	C.G.I.	
	GUARDIA CIVIL	
	AGENCIA ESPAÑOLA PR. DATOS	
	Cª GRAL. POLICÍA JUDICIAL	
	D.G.P	
FR	Direction générale de la police nationale (DGPN)	20/03/2012
	Direction centrale de la police judiciaire (DCPJ) – division des relations internationales (DRI) – DAPIX	

	Direction centrale de la police judiciaire (DCPJ) – division des relations internationales (DRI) et section centrale de coopération opérationnelle de police (SCCOPOL)	
	Direction centrale de la police judiciaire (DCPJ) – sous-direction de la police technique et scientifique (SDPTS)	
	Direction centrale de la sécurité publique (DCSP) - sous-direction des missions de sécurité, division des activités judiciaires (SDMS – DAJ)	
	Direction de la coopération internationale (DCI)	
	Service des technologies et des systèmes d'information de la sécurité intérieure (STSI^2) - sous-direction des systèmes d'information (SDSI)	
EE	Ministry of Justice	22/03/2012
	Centre of Registers and Information Systems	
	Estonian Ministry of Interior	
	The Office of the Prosecutors General	
	Estonian Tax and Customs Board	
	IT and Development Centre. Ministry of the Interior	
	Police and Border Guard Board	
	The Data Protection Inspectorate	
SE	Division for Investigations & Proceedings, NPB	29/03/2012
	NPB	
	Division for Crime Prevention, NPB	
	IPO Front Office at the National Bureau of Investigation, NPB	
	Department for Information Technology, NPB	
	Ministry of Justice	
	Swedish Customs	
	Swedish data protection authority	

Organisations represented during meetings with experts:

Meeting date	MS/Organisation	Description
30/01/2012; 23/02/2012	Europol	Discussion on experience related to Europol Information System, Siena, EIXM and target IM architecture, UMF 2 and Information exchange platform in the context of EPRIS
19/04/2012	AT, BE, CZ, CY, DE, DK, ES, EE, FI, FR, EL, HU, IE, IT, LT, LU, LV, MT, NL, PL, RO, SI, SE, UK EDPS EUROPOL GSC	Expert meeting on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records Index System (EPRIS)

Annex 5: Summarised records of meetings with Member States and other stakeholders

This annex includes interview highlights related to completed country visits and the mission to Europol.

Information contained in this annex is confidential.

Annex 6: Description of scenarios

EUROPEAN POLICE RECORD INDEX SYSTEM (EPRIS)

DESCRIPTION OF SCENARIOS

TABLE OF CONTENTS

1 Acronyms and abbreviations

Acronym or Abbreviation	**Meaning**
DB	Database
EPRIS	European Police Record Index System
IT	Information Technologies
MS	Member State
s-TESTA	secure Trans-European Services for Telematics between Administrations

2 Introduction

This document presents the main policy options for the development of a European Police Record Index System (EPRIS). For each option, it outlines the key implications in terms of management structure, costs/benefits, legal implications and information technology.

Overall, 4 different options will be looked into:

EPRIS scenarios	No new system	Centralised	Semi-centralised	Decentralised
Reference no	0	1	2	3

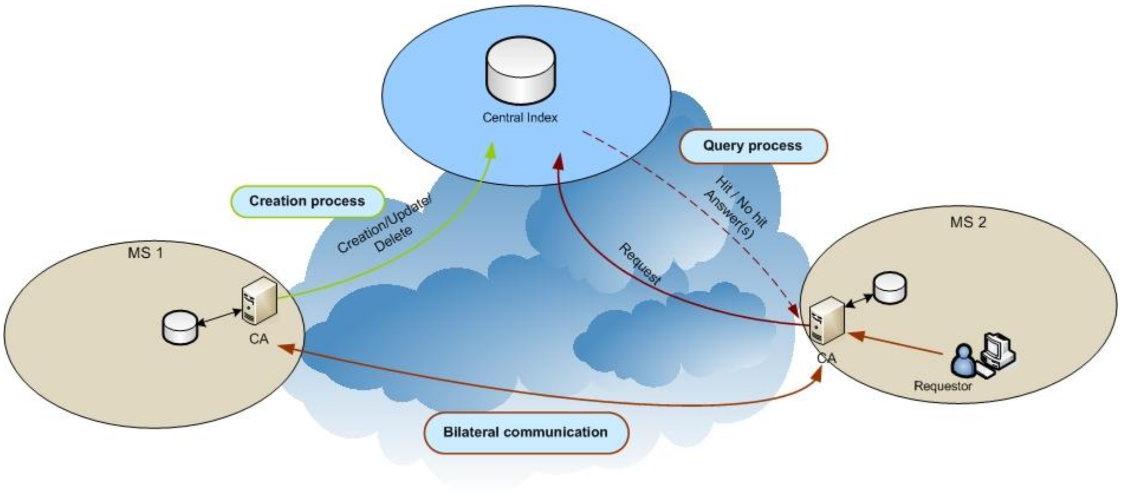
3 Baseline scenario: No New System

The baseline scenario corresponds to a situation where no further action is taken at EU level regarding the exchange of information between police and other law enforcement authorities for the purpose of criminal investigation. This would also imply that no specific management structure would need to be put in place at EU- or national level, other than what is currently foreseen, and no new legal instrument would be required. The existing IT channels would continue to be used which means that no additional costs would be incurred for a development of an Index. However, this solution includes the shortcomings of the current information exchange where no possibility exists for MS' law enforcement authorities to have a quick overview of whether and possibly where relevant information on a certain person can be found.

4 Possible architectural approaches

4.1 Centralised System

A Central Index would function as a hit/no hit system with a central storage system that would include the information necessary to find out whether other MS hold information on the person concerned. The Index would function as a tool that would instantly point the authority that performs a query towards the MS keeping relevant information. Only the minimum amount of data that is available in all MS and ensures a reliable identification and matches the query will be stored on the Index. Once a person has been clearly identified, subsequent exchanges of information can take place bilaterally. This approach is illustrated in the figure below.



4.1.1 Management Structure

1) EU Level: For the management of a centralised system, a single management body at EU level, with the responsibility of ensuring efficient EU-wide searches and information exchanges, seems to be the logical approach. A dedicated management team in charge of the operations would guarantee a high level of service availability and would provide its support to new countries joining the network. This institution would have an operational support role ***but would not have access to the information contained in the Index and exchanged between MS.*** The central management authority would also be responsible for setting up an adequate monitoring mechanism. This would include gathering relevant statistics in order to monitor the fulfillment of operational objectives of the EPRIS.

2) MS Level: It is assumed that one authority dealing with criminal investigation would be in charge of processing requests, creating, updating or deleting information in the Index.

4.1.2 Costs/Benefits

The main benefit of the Central Index is the higher level of automation that is possible because of the centralisation of key data. The advantages related to the data protection aspect should also be mentioned, since the central system allows for having the logging functionality for requests and setting controls at the central level.

4.1.3 Legal implications

This option will require a new legal instrument at EU level to provide a sound legal basis.

4.1.4 IT

The data stored centrally must represent the minimum necessary information for identifying a person (e.g. passport number, nationality, name, first name, place of birth and date of birth). Additional information filtering through other fields (alias, …) could increase the overall accuracy rate.

The advantages of a central Index from an IT perspective are:

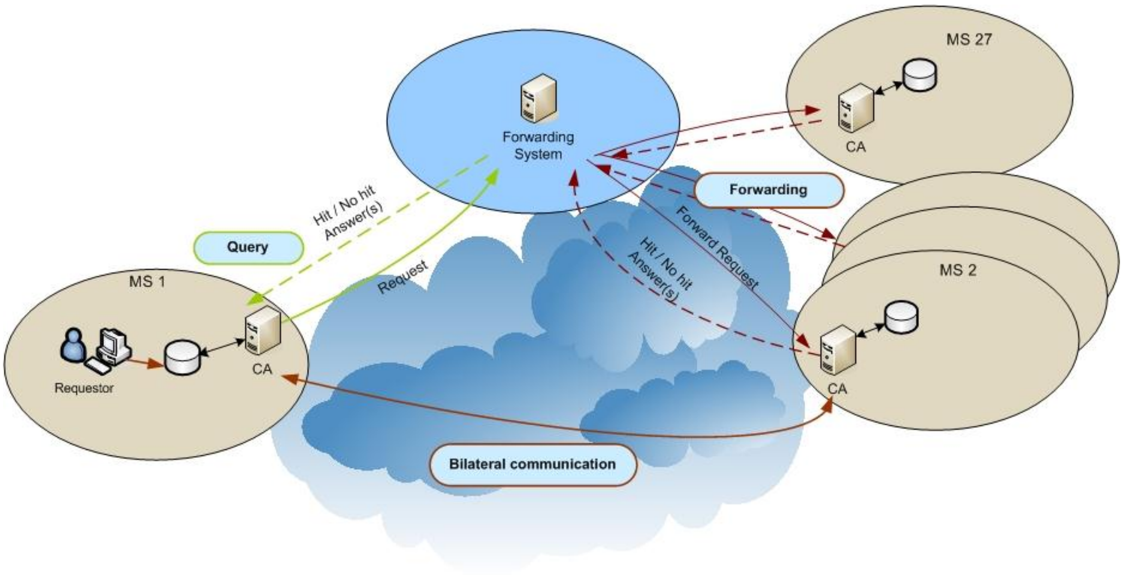
- Testing of the application implementation is only necessary between each MS and the Index. Bilateral testing between MS is not needed.
- As the Index will be regularly updated by the MS, all queries will receive a hit/no hit reply in real time without having to wait for an acknowledgement by all MS.
- A centralised management of services as helpdesk, support, development and availability would be easier.
- There can be a common interface tool for all MS.
- There can be a common search tool.

One potential issue of this solution relates to the hosting of the Index, but in any case the following functional safeguards should be enforced:

- Each MS would have a reserved area in the Index and would be responsible for the data stored in this area. The ownership of the data would remain within the MS that created it. That means that only this MS would have the right to administer and directly access the data (i.e. no browsing from another MS).
- A query from a requester should check all the records of the Index without any restriction. That means that the owner of the data should not be able to “hide” any records.
- The administrator of the Index should not have access to any data belonging to the MS.
- Technical, organisational and procedural measures should be enforced to guarantee confidentiality, integrity and availability of the data exchange. This could be implemented by using encryption and message signature.

4.2 Semi-Centralised System

A semi-centralised system would be a hit/no-hit system without central data storage. This option represents a central server for relaying queries from requesting countries to receiving countries. The server would only relay messages and the data would not be stored in the server. The server could log queries to monitor data quality and integrity as well as introduce time stamps. It would also return the hit /no hit responses to the requesting Member State. These responses would, in case of a hit, contain contact information for requesting the content of the hit. Subsequently, bilateral exchanges of information would take place while using existing channels. The approach is illustrated in the figure below.



4.2.1 Management Structure

1) EU Level: A specific team in charge of the operations will be established to guarantee a high level of service availability and provide assistance to new countries joining the network. This institution would have an operational support role. It would also act as an auditor and would ensure the provision of reliable statistics.

2) MS Level: It is assumed that one authority dealing with criminal investigation would be in charge of creating and processing the requests.

4.2.2 Costs/Benefits

The main benefit of the semi-central system is the higher automation at the central server level. However, since the requests will be broadcasted in a decentralised way and will have to be processed by 26 MS. Drawbacks in terms of time and workload should be considered.

4.2.3 Legal implications

This option will require a new legal instrument at EU level to provide a sound legal basis.

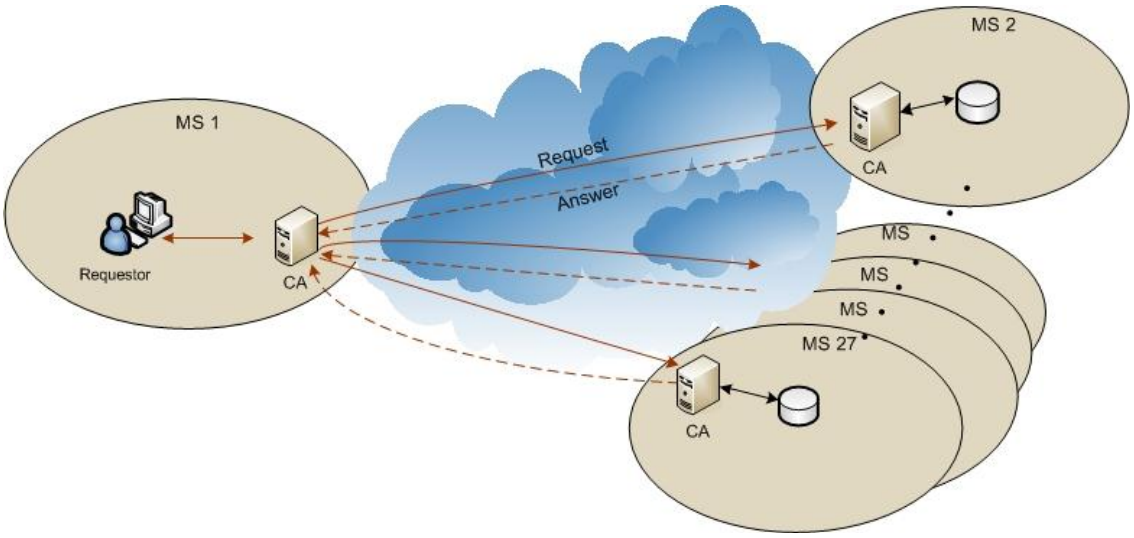
4.2.4 IT

The advantages of a semi-central system from an IT perspective are:

- Testing of the application implementation should only be done between each MS and the forwarding system.
- A centralised management of services as helpdesk, support, development and availability would be easier.

4.3 Decentralised System

This solution does not imply the development of a central index or storing data at European level. Each request initiated by a MS will be broadcasted to all the other MS that will send back the information, if any. This solution is depicted in the figure below.



4.3.1 Management Structure

1) At EU level: No additional central management structure is required

2) At MS level: Expert groups responsible for the technical and legal questions might need to be established that would meet on a regular and ad hoc basis before and after the system becomes operational. The technical working group would determine the technical specifications whereas the legal working group would develop the legal guidelines. It is assumed that a committee will be established to ensure the coordination between the MS.

4.3.2 Costs/Benefits

The main benefit of this approach is that this option enables the exchange of information without having to develop a new Index and storing information centrally. However, drawbacks might appear on a performance level (both technically as well as in terms of complexity of the management processes). A major cost related to this option can be measured in terms of time needed for MS to handle each request, as they will receive every single request sent by any of the MS. Each request from a MS will have to be processed by the 26 other MS. Assuming that this process is not fully automated for all MS, the multiplication of the number of requests will generate a substantial additional workload for these countries.

4.3.3 Legal implications

This option is likely to require a new legal instrument at EU level to provide for a sound legal basis.

4.3.4 IT

This solution is described as a full mesh infrastructure with no information stored centrally. The number of interfaces would be quite high. This would be achievable if an interoperability standard is developed and adopted. Infrastructures of this nature are supported by sTesta and are already used for other existing systems at EU level (such as FIU.NET or EUCARIS). A request is sent to all 26 MS, which check records in their relevant information systems and then send a reply.

The use of web services combined with common reference tables does not require adjustments of the architecture at national level, as long as the countries have computerised records systems connected to a common secure network. Changes to a national database may however make the database of this country temporarily unavailable through these web services. Availability may therefore be an issue. In a full meshed configuration might lead to an incomplete overview as long as some MS have not responded to the query. Another drawback of a full meshed configuration concerns the testing of the application implementation, which has to be done between the 27 MS.

Annex 7: Main study instruments

7.1 Questionnaire

QUESTIONNAIRE FOR THE STUDY "EUROPEAN POLICE RECORDS INDEX SYSTEM (EPRIS)"

COUNTRY REPORT: ENTER COUNTRY NAME

Table of contents

1 Introduction

According to the Stockholm Programme, the Commission has to carry out a feasibility study on the need for, and the added value of setting up a European Police Records Index System (EPRIS) and to present a report to the Council in the course of 2012.

In order to prepare this report, the Commission has tendered a study on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records Index System (EPRIS). Between January and March 2010, a pre-study on the need for a European Police Records Index System (EPRIS) was conducted by the Commission.

On 14th October 2011, the Commission contracted UNISYS Belgium and the Institute for International Research on Criminal Policy (IRCP) Ghent to conduct the EPRIS study. The study will inter alia evaluate the current context in the Member States, look into possible ways of providing a definition of the term "police record" at EU level and assess possible options for a European Index System. As a system with only alphanumeric data does not always allow an unequivocal identification of a person, the additional use of biometric data should also be considered. Both centralised and decentralised scenarios will be examined taking into account already existing information management systems, such as the Europol Information System, Prüm or Customs files identification database (FIDE). It will also take into account the principles and focus areas of the EU Information Management Strategy for EU internal security[31].

1.1. Assumptions

Basic assumptions were made when designing this questionnaire:

1. There will be a legal framework in place to support EPRIS.
2. In the exchange of information, safeguards will be in place to ensure alignment with existing information exchange mechanisms, policies and cooperation channels.
3. The security architecture will be compliant with the confidentiality levels of the information involved.
4. Relevant data sources will run on interconnected networks.
5. Identity and access management arrangements will be in place.
6. Supervisory authorities will be defined and will have access to security and data protection audit logs.
7. Conditions/restrictions imposed for the handling of information will be respected as part of the processing.

Please indicate in the box below, any relevant comments on these assumptions:

Member State comments on the assumptions

[31] Council Conclusions on an Information Management Strategy for EU internal security, 2979 JHA Council meeting, 16637/09 JAI 874 CATS 131 SIM 137 justciv 249 JURINFO 145, 30.11.2010.

1.2 How to complete this questionnaire

This questionnaire aims at gathering facts in order to assess the current situation in EU Member States regarding the information exchange for criminal investigation purpose as well as their view on the possible establishment of a European Police Records Index System. Similarly, the issue of the definition of the police record will be addressed.

Since the scope of *the study is limited to the criminal investigation area* and does not include administrative policing, the appointed Single Point of Contact (SPOC) should identify *all relevant law enforcement authorities* which deal with such type of information at national level. As such, the stakeholders' engagement should not be narrowed down to police authorities only but should concern all other actors involved in criminal investigation procedures at national level (e.g. inspection services, customs, etc.).

Due to specific questions included in the questionnaire, it is recommended to also consult the authorities managing the national fingerprints database and data protection authorities.

For this purpose, the questionnaire *is sent to the SPOC in each of the Member States, who will then dispatch the different questions amongst his identified competent authorities*. It is suggested that a meeting is held by the SPOC to coordinate and consolidate answers received from different stakeholders at national level.

The questions are divided into two main sections:

Section 2.1: Current situation regarding information exchange for criminal investigation purpose at national level. This section includes questions on:

- ***Section 2.1.1: Information available at national level*** includes questions on the content of a record as well as ICT aspects of the national records information system(s) used by police and other law enforcement authorities.

- ***Section 2.1.2: Current exchange of information*** covers procedural and legal aspects involved in the exchange of records information.

Section 2.2: Member States' views on the possible establishment of a European Police Records Index System. The questions concern:

- ***Section 2.2.1: Scope of the system*** *includes questions on information that should be made available via EPRIS.*

- ***Section 2.2.2: Architectural and legal aspects of EPRIS**:* concerns organisational, ICT and legal aspects of a possible Index system.

As a SPOC, you are kindly requested to coordinate the input from the different competent authorities and return the completed questionnaire to UNISYS.

Thank you beforehand for your help.

1.3 Important notice

For further enquiries regarding the project in general or this questionnaire, feel free to send a mail to the following mailbox: EPRIS@unisys.com

Please replace the "XX" in the filename by the ISO 3166-1-alpha-2 country code[32] (e.g. BE for Belgium) when saving the file and send the completed questionnaire back to EPRIS@unisys.com

[32] Complete list available on http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm

Please indicate by checking the appropriate box below whether you accept that this questionnaire, once completed, be posted on CIRCA-BC[33]:

□ Yes
□ No

[33] CIRCA-BC is a portal developed under the European Commission IDA programme. It enables collaborationbetween the European Institutions and the Public Administration.

2 Questions

2.1 Current situation regarding information exchange for criminal investigation purpose at national level

2.1.1 Information available at national level

2.1.1.1 In your country, what information is contained in your records information system(s) used for criminal investigation purposes by police and other law enforcement authorities?

Person related information

□ Surname

□ First name(s)

□ Surname at birth, if different

□ Alias

□ Gender

□ Nationality

□ Date of birth

□ Place of birth

□ Father's name

□ Mother's name

□ Residence or known address

□ Fingerprint template

□ Fingerprint image

□ DNA

□ Palm prints

□ Photo/facial recognition

□ Scars, marks and tattoos

□ Other. Please specify:

Legal person related information

□ Legal Name

□ Shortened name/common name

□ Country of Incorporation

□ Register and/or number of legal person

□ Address of registered office

□ Name of legal representative

Objects/events related information

□ Type of offence

□ Date of offence

□ Vehicle registration data

□ Telephone number

□ Bank account number

□ Criminal records information
(information on prior convictions by court)

□ Criminal organisation (name)

□ Type of drugs

□ Firearm information (type/serial number)

□ Means of communication

□ Means of transportation

□ Place of crime scene

□ Other: Please specify:

Could you describe how the information enlisted above is stored in your country?

□ In one system

□ In separate systems for different purposes

If relevant, more information on the general setup could be provided in questions 2.1.1.5 and 2.1.1.6 of this questionnaire.

2.1.1.2 To which categories of persons does the information stored in your records information system(s) relate?

□ Suspected persons
□ Perpetrators (labelled as guilty by law enforcement authorities)
□ Convicted persons (found guilty by court)
□ Detainees
□ Associates
□ Witnesses
□ Victims
□ Others. Please specify:

Is this information stored as a specific field in the records?

□ Yes
□ No

2.1.1.3 Do your records include information on the quality of the data which helps to clarify whether the data to be exchanged are hard facts or suspicions?

□ Yes.

Do you use fields to specify whether the information is:

□ Reliable

□ Police found evidence

□ Anonymous testimony

□ Other (e.g. grading system). Please specify:

□ No

2.1.1.4 Can you provide a definition for what is considered a 'police record' in your country?

□ Legal definition. Please provide the source, if applicable:

Definition:

□ Functional definition. Please provide the source, if applicable:

Definition:

□ No definition

Reason:

Note: Please add definitions of a 'record' and the source used by each relevant law enforcement authority in your country, if applicable:

2.1.1.5 Could you summarise briefly the organisational aspect of the storage of information used for criminal investigation purpose in your country?

□ Do you have a centralised records information system used by police and other relevant law enforcement authorities?

□ Yes

Please specify the name of the authority managing the system:

Please specify the information system name:

What is the level of automation?

□ Fully automated

□ Partly manual (i.e. certain function(s) being operated by hand). Please specify:

□ Fully manual (i.e. based on paper files only)

Which authorities have access to the centralised records information?

□ Police

□ Border Guard Service

□ Financial Crime Investigation Service

□ Other. Please specify:

□ No, there is no centralised records information system used by police and other relevant law enforcement authorities in our country

Are there legal obstacles for establishing a centralised records information system?

□ Yes. Please specify:

□ No

Please summarise briefly the different records information systems used by police and other law enforcement authorities involved in criminal investigation procedures:

Managing authority	Information system name	Automation level (A – fully automated; M – partly manual; F – fully manual)

Please explain whether these systems are interconnected?

□ Yes. Please specify:

□ No

2.1.1.6 Does/do your records information system(s) used for criminal investigation purpose include fingerprints?

□ Yes

Please specify the information system name:

What is currently the percentage of persons available in your records for whom there is fingerprint information available?

□ No

If No

Are there any legal obstacles for including fingerprints in your records database(s)?

□ Yes. Please specify:

□ No

Is there a link to a national fingerprint database (AFIS)?

□ Yes

□ No. Are there any plans to create such a link?

□ Yes. Please specify timeframe :

□ No

Are there any plans to include the fingerprints in your records database(s)?

□ Yes. Please specify timeframe :

2.1.2 Current exchange of information

2.1.2.1 Please describe the most typical scenarios in which an authority dealing with criminal investigation in your country needs access to information contained in records from other EU Member States (who needs what exactly, under which circumstances?)
2.1.2.2 Please describe the typical level at which the access to information is required mostly at national level?
□ Patrol officer on street □ Investigating officer □ Other. Please specify:

2.1.2.3 When you need to check whether there is relevant information available in other Member States in the course of a criminal investigation, which of the following channels do you currently use? Please indicate their usefulness and provide details.		
	Particularly useful (please specify why)	Less useful (Please specify why)
□ Europol information system		
□ Schengen information system (SIS)/SIRENE		
□ Prüm		
□ European Criminal Record Information System (ECRIS)		
□ Customs files identification database (FIDE)		
□ Interpol		
□ Police and customs cooperation centres (PCCC)		
□ Other systems. Please specify:		

2.1.2.4 In order for us to prepare recommendations on the most appropriate EPRIS approach, we need to consider the cost impact but we would like to avoid requesting detailed cost impact estimations from you at this stage. Could you provide us with cost estimates/reports for the implementation work at the national level regarding the following large-scale information systems? (Please note that this information will not be published or used for comparison purposes)

□ Europol information system
□ Schengen information system (SIS)
□ European Criminal Record Information System (ECRIS)
□ Prüm
□ Customs files identification database (FIDE)
□ Other. Please specify:

2.2. Member State's view on the possible establishment of EPRIS

2.2.1 Scope of the system

2.2.1.1 Which criteria do you consider as necessary to conduct a search via EPRIS in order to identify whether information on a certain person required for criminal investigation purposes is held in other EU Member State(s)?

Criterion	**Essential**	**Less useful**
Person related information		
Surname	□	□
First name(s)	□	□
Surname at birth, if different	□	□
Alias	□	□
Gender	□	□
Nationality	□	□
Date of birth	□	□
Place of birth	□	□
Father's name	□	□
Mother's name	□	□
Residence or known address	□	□
Fingerprint template	□	□
Fingerprint image	□	□
DNA	□	□
Palm prints	□	□
Photo/facial recognition	□	□
Scars, marks and tattoos	□	□
Other. Please specify:	□	□
Legal person related information		
Legal Name	□	□
Shortened name/common name	□	□
Country of Incorporation	□	□
Register and/or number of legal person	□	□
Address of registered office	□	□

Name of legal representative	□	□	
Objects/events related information			
Type of offence	□	□	
Date of offence	□	□	
Vehicle registration data	□	□	
Telephone number	□	□	
Bank account number	□	□	
Criminal records information (information on prior convictions by court)	□	□	
Criminal organisation (name)	□	□	
Type of drugs	□	□	
Firearm information (type/serial number)	□	□	
Means of communication	□	□	
Means of transportation	□	□	
Place of crime scene	□	□	
Other: Please specify:	□	□	

Please select one of the following:

□ The scope of the search should be limited to manual searches (i.e. warning you whether or not there is a hit in the index on the data used to perform a direct query on the index)

□ The scope of the search should also include the possibility of automated cross-checks (i.e. warning you automatically whether or not there is a hit in the index on the data you have inserted in your own records information system)

Would you find it useful to make a search based on combined criteria in case of the multiple hits?

□ Yes. Please specify:

□ No

Please list the reasons for either supporting or opposing the use of fingerprints to search in the European Index:

Supporting:

Opposing:

2.2.1.2 On which categories of persons should EPRIS be searchable?

□ Suspected persons
□ Perpetrators (labelled as guilty by law enforcement authorities)
□ Convicted persons (found guilty by court)
□ Detainees
□ Associates
□ Witnesses
□ Victims
□ Others. Please specify:

**2.2.1.3 Do you prefer to receive information as hit/no-hit information only?
Remark: a hit could mean the identification of the Member State(s) holding a certain piece of information required for the criminal investigation purpose in the requested Member State**

□ Yes, that would suffice.
□ No, additional information would be welcome:

□Type of offence related to the hit.

The EU level offence classification system (EULOCS) has been recently developed which enables one to understand which crime has been committed in another Member State, even though definitions and language among Member States defer. Would you find it useful to use EULOCS as a reference system?

□ Yes
□ No. Please specify why not:

□ Description of responsible authority
□ File number of the authority
□ Date of offence related to the hit
□ Other. Please specify:

2.2.1.5 Is it necessary to include in the European Index information related to all offences or only to a limited number of offences?

□ All offences should be included.

□ Only certain types of offences should be included (e.g. offences mentioned in the European Arrest Warrant, limited selection of offences from ECRIS list, offences falling within EUROPOL mandate, etc.). Please specify:

2.2.2 Architectural and legal aspects of EPRIS

2.2.2.1 Please indicate your preference, if any:

□ Centralised system: central storage server with minimum amount of data from Member States databases necessary to receive a hit
□ Semi-central system: central server only for relying queries from requesting country to receiving countries without storage of data on the server (the hub-and-spoke model). In this scenario, Member States do not send a request to all other Member States directly themselves, they send one request to the central server.

□ Decentralised system: information broadcast from one Member State to all Member States in order to receive a hit without any central element involved
□ No preference
□ Other. Please specify:

2.2.2.2 Please list the reasons for either supporting or opposing the use of centralised, semi-centralised or decentralised architecture for EPRIS

	Pros	**Cons**
Centralised system		
Semi-central system		
Decentralised system		

2.2.2.3 What, if any, would be the most important obstacles in your country for setting up a new European index system for criminal investigations related information exchange?

□ legislative obstacles
□ data protection issues
□ costs
□ technical structure (including interfaces to national data systems and the possible data transfer from national systems to the index system)
□ organisation and management
□ timetable
□ practical use (e.g. access to/user of the system; search methods, translation)
□ others. Please specify:

Please provide more details on the additional burden the establishment of a European index system for criminal investigations related information exchange would create on your national administration:

2.2.2.4 Compliance with the established data protection principles is one of the core aspects of the EPRIS study. Which of the following elements should, in particular, be looked at when considering the structure, functions and scope of EPRIS?

□ Necessity

□ Proportionality

□ Subsidiarity

□ Purpose limitations

□ Rectification

□ Erasure or blocking

□ Limited time of data storage

□ Verification of data quality (reliability, accuracy, correctness, currency, completeness and relevance)

□ Identification of data recipients

□ Data ownership (different treatment of information collected by a Member State or received from another Member State)

□ Access limitations and access control

□ Confidentiality

□ Other. Please specify:

Please indicate the elements that are of extraordinary importance regarding specific categories of persons concerned, such as suspects or witnesses:

2.2.2.5 What should be the access rights given to different stakeholders?

Stakeholder	Access mechanism
Patrol officer	□ No access □ Direct access □ Through a central authority
Criminal investigation officer	□ No access □ Direct access □ Through a central authority
Border guard service/customs	□ No access □ Direct access □ Through a central authority
Inspection service	□ No access □ Direct access □ Through a central authority
Prosecution service	□ No access □ Direct access □ Through a central authority
Others (e.g. judiciary, penal institution). Please enlist:	□ No access □ Direct access □ Through a central authority
Data subject (for the purpose of consulting the data to control/rectify it)	□ No access □ Direct access □ Through a central authority

2.2.2.6 Should EU agencies have the right to search EPRIS for information that falls under their mandate (e.g. Europol, Eurojust, Frontex, OLAF)

□ Yes

□ No

Please explain:

End of questions – Thank you for your answers

7.2 Interview Guide

INTERVIEW GUIDE FOR THE STUDY "EUROPEAN POLICE RECORDS INDEX SYSTEM "

ENTER COUNTRY NAME

Table of contents

1 Introduction

1.1. Background

According to the Stockholm Programme, the Commission is called upon to carry out a feasibility study on the need for, and the added value of setting up a European Police Records Index System (EPRIS) and to present a report to the Council in the course of 2012.

In order to prepare this report, the Commission has tendered a study on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records Index System (EPRIS). Between January and March 2010, a pre-study on the need for a European Police Records Index System (EPRIS) was conducted by the Commission.

On 14th October 2011, the Commission contracted UNISYS Belgium and the Institute for International Research on Criminal Policy (IRCP, Ghent University) to conduct the EPRIS study. The study will inter alia evaluate the current context in the Member States, look into possible ways of providing a definition of the term "police record" at EU level and assess possible options for a European Index System. As a system with only alphanumeric data does not always allow an unequivocal identification of a person, the additional use of biometric data should also be considered. Both centralised and decentralised scenarios will be examined taking into account already existing information management systems, such as the Europol Information System, Prüm or Customs files identification database (FIDE). It will also take into account the principles and focus areas of the EU Information Management Strategy for EU internal security[34] and the principles set out in the Commission's 2010 Communication[35].

1.2. How to use this Interview Guide

This Interview Guide will be used as a support for the face-to-face meetings taking place in the Member States. It will ensure that all key issues are addressed systematically in order to guarantee the comparability of the results across the Member States.

It can be used by the Single Points of Contacts appointed for this study to prepare for these meetings, to gather relevant documentation or to organise preparatory meetings with the competent national authorities. The outcome of such preparatory discussions should be used to pre-fill this interview guide prior to the meeting. It will also be used by the Consultants during the meeting itself as an information collection tool.

It also contains a standard structure for the meeting agenda. This can however be adjusted on an ad-hoc basis upon suggestion from the Single Point of Contact. He or she has a better understanding of the national context and can ensure the project takes national specificities into consideration (e.g. need to visit authorities located in different cities, etc).

1.3. Permission for information sharing

□ The Member State agrees that the completed Interview Guide can be published as a mission report on CIRCA *(Please tick the box to indicate agreement)*

[34] Council Conclusions on an Information Management Strategy for EU internal security, 2979 JHA Council meeting, 16637/09 JAI 874 CATS 131 SIM 137 justciv 249 JURINFO 145, 30.11.2010.

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

2 Date - place – participants

2.1 Date and place of the meeting(s):

2.2 Meeting Participants

Name	First Name	Institution	Address	Email	Phone

This table is not limitative regarding the number of participants and can be expanded

3 Meeting Agenda

3.1 Introduction of Meeting Participants

Suggested duration: 30 min

At the start of the meeting, all participants present themselves, their particular background, expertise and the authorities they represent.

3.2 Presentation of the study

Suggested duration: 30 min

The study team members provide an overview of the study context, objectives and the expected outcome. The project team, the planning of the project and its current status are presented to the meeting participants.

3.3 Current situation regarding the exchange of police records information

Suggested duration: 120 min

Member States' experts are requested to prepare a presentation that provides an overview of the content of their different law enforcement records, its use during criminal investigations and the key characteristics of law enforcement records information exchange in their country. It is a good occasion to highlight particular concerns or good practices at national level regarding the exchange of law enforcement records information and the presentation may include an on-site visit and a short demonstration of the systems in use.

To the extent possible, this presentation will also address the requests for additional information on the Questionnaire enlisted below (boxes are available below each question to provide clarifications):

Questions on answers provided to the Questionnaire:

- Question that requires further clarification (to be completed after analysis of the Questionnaire Responses)

- Question that requires further clarification (to be completed after analysis of the Questionnaire Responses)

- Question that requires further clarification (to be completed after analysis of the Questionnaire Responses)

- Question that requires further clarification (to be completed after analysis of the Questionnaire Responses)

- Question that requires further clarification (to be completed after analysis of the Questionnaire Responses)

- Question that requires further clarification (to be completed after analysis of the Questionnaire Responses)

Notes on the Member State’s presentation(s):

3.4 Discussion on the definitions of police record

Suggested duration: 20 min

This part of the meeting gives Member States a chance to express their opinion on the proposed definitions of 'police record' or 'law enforcement record' (Annex I).
Member states can elaborate what they think of:

1) A more general definition (e.g. the national register or registers recording data of law enforcement authorities for criminal investigations), leaving the interpretation of the appropriate records up to the member states.
2) An elaborate definition, limiting EPRIS' records on the following aspects:
   - the law enforcement authorities whose records are searched through EPRIS
   - the criminal offences for which EPRIS should be used
   - the categories of persons whose information can be searched (suspects, victims, witnesses, etc.)
   - limiting the criteria for which can be searched (names, date and place of birth, nationality, etc.)

Member States' experts can bring forward arguments supporting either option. The choice should not per se be made between option 1 or 2, rather the advantages/disadvantages of all options/aspects should be clarified.
Due consideration should be given to the following aspects: the finality of the information to be queried through EPRIS (e.g. the use for criminal investigations) and the criteria contained into the different records (e.g. name, date, fingerprints, previous convictions…).

3.5 Discussion on the different options for a European Police Records Index System (EPRIS)

Suggested duration: 120 min

This part of the meeting aims at assessing the view of Member States' experts on the impacts, the pros and cons of the different scenarios under consideration for EPRIS.
It is suggested that the representatives of the Member State give a presentation of arguments in favour of a specific scenario(s) (Annex I). To support the discussion with the Member States, the Unisys team members will use a presentation describing potential implications of different scenarios and asking key questions in order to assess the importance of such impacts.

As a second step, a more detailed analysis will be undertaken in order to receive Member States' opinion on the following specific issues:

- Management Structure – Organisational and Institutional aspects
- Process for Creation, Update, Deletion and Search of the index
- Application and data structure
- Communication Network
- Security controls and requirements
- Legal, social and political aspects
- Data protection aspects/requirements
- Costs and Benefits

4 Interview summary and conclusions

The meeting will be finalised by drawing the key points and summarising the main findings.

Key points and findings

Annexes

ANNEX I: Proposed definitions of ‘police record’

EUROPEAN POLICE RECORD INDEX SYSTEM (EPRIS)

DESCRIPTION OF ‘POLICE RECORD’ DEFINITIONS

1. Introduction

This document presents the main options on a definition for 'police records'. For each option, it outlines the key features in terms of scope.

Overall, the different options can be summarised as such:

1) A more general definition (e.g. the national register or registers recording data of law enforcement authorities for criminal investigations), leaving the interpretation of the appropriate records up to the member states.

2) An elaborate definition, limiting EPRIS' records on the following aspects:

   - the law enforcement authorities whose records are searched through EPRIS
   - the criminal offences for which EPRIS should be used
   - the categories of persons whose information can be searched (suspects, victims, witnesses, etc.)
   - limiting the criteria for which can be searched (names, date and place of birth, nationality, etc.)

2. A general definition:

A 'Police Record' shall mean the national register or registers recording data of law enforcement authorities for the prevention, detection, investigation and prosecution of criminal conduct, the latter being defined by national law.

Features:

- Not limited to police authorities, but all law enforcement authorities working with a criminal justice finality. EPRIS is thus conceived as a 'European Criminal Investigation Record Index System', rather than a 'European Police Record Investigation Record'. Instead of looking at the source of information, the finality of the information is important. This leads to the exclusion of administrative policing and intelligence authorities, however including customs, border guard services and others.

3. Limitations to a general definition

A. Concerning the law enforcement authorities

A 'Police Record' shall mean the national register or registers recording data of *police authorities and/or gendarmerie and/or customs and/or border guard services and/or financial crime unit (*)* for the prevention, detection, investigation and prosecution of criminal conduct, the latter being defined by national law.

(*) preferences to be indicated and substantiated. Choices can be expanded.

Feature:

- While conducting a criminal investigation, EPRIS can only be used to search the databases of the chosen law enforcement authorities.

B. *Concerning the criminal offences to be covered*

A ‘Police Record’ shall mean the national register or registers recording data of law enforcement authorities on *Europol crimes*[36] *or European Arrest Warrant crimes*[37] *or crimes punishable with a custodial sentence of at least x months or (*)* for the prevention, detection, investigation and prosecution of criminal conduct, the latter being defined by national law.

(*) preferences to be indicated and substantiated. Choices can be expanded.

Feature:

- EPRIS could be set up to check during a criminal offence whether there is information in another member state on any person/object/event/location. However, Member States might want to limit those checks to certain criminal offences.

[36] Art. 4 of Council Decision 2009/371/JHA establishing the European Police Office (Europol), *OJ L 121*, 15.5.2009: “organised crime, terrorism and other forms of serious crime as listed in the annex” (unlawful drug trafficking, illegal money-laundering activities, crime connected with nuclear and radioactive substances, illegal immigrant smuggling, trafficking in human beings, motor vehicle crime, murder, grievous bodily injury, illicit trade in human organs and tissue, kidnapping, illegal restraint and hostage taking, racism and xenophobia, organised robbery, illicit trafficking in cultural goods, including antiquities and works of art, swindling and fraud, racketeering and extortion, counterfeiting and product piracy, forgery of administrative documents and trafficking therein, forgery of money and means of payment, computer crime, corruption, illicit trafficking in arms, ammunition and explosives, illicit trafficking in endangered animal species, illicit trafficking in endangered plant species and varieties, environmental crime, illicit trafficking in hormonal substances and other growth promoters).

[37] Art. 1 of Council Framework Decision on the European arrest warrant and the surrender procedures between Member States. “Acts punishable by the law of the issuing Member State by a custodial sentence or a detention order for a maximum period of at least 12 months or, where a sentence has been passed or a detention order has been made, for sentences of at least four months; or the following offences, if they are punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined by the law of the issuing Member State” (participation in a criminal organisation, terrorism, trafficking in human beings, sexual exploitation of children and child pornography, illicit trafficking in narcotic drugs and psychotropic substances, illicit trafficking in weapons, munitions and explosives, corruption, fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests, laundering of the proceeds of crime, counterfeiting currency, including of the euro, computer-related crime, environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties, facilitation of unauthorised entry and residence, murder, grievous bodily injury, illicit trade in human organs and tissue, kidnapping, illegal restraint and hostage-taking, racism and xenophobia, organised or armed robbery, illicit trafficking in cultural goods, including antiques and works of art, swindling, racketeering and extortion, counterfeiting and piracy of products, forgery of administrative documents and trafficking therein, forgery of means of payment, illicit trafficking in hormonal substances and other growth promoters, illicit trafficking in nuclear or radioactive materials, trafficking in stolen vehicles, rape, arson, crimes within the jurisdiction of the International Criminal Court, unlawful seizure of aircraft/ships, sabotage).

C. Concerning the categories of persons whose information is checked

A ‘Police Record’ shall mean the national register or registers recording data of law enforcement authorities on *suspects and/or perpetrators and/or convicts and/or detainees and/or associates and/or witnesses and/or victims (*)* for the prevention, detection, investigation and prosecution of criminal conduct, the latter being defined by national law.

(*) preferences to be indicated and substantiated. Choices can be expanded.

Feature:

- A search through EPRIS might be limited to certain categories of persons. For instance, a Member State might be of the opinion that searching for information on witnesses is irrelevant for criminal investigations.

D. Concerning search criteria

A ‘Police Record’ shall mean the national register or registers recording data of law enforcement authorities for the prevention, detection, investigation and prosecution of criminal conduct, the latter being defined by national law. It shall contain only data on the following particulars: *surname and/or first name and/or alias and/or gender and/or nationality and/or date of birth and/or name of father and/or name of mother and/or residence or known address and/or fingerprints and/or DNA and/or palm prints and/or photo and/or scars, marks and tattoos and/or name of legal entity and/or shortened name of legal entity and/or country of incorporation of the legal entity and/or register number of legal entity and/or address of legal entity and/or name of legal representative and/or type of offence and/or date of offence and/or vehicle registration data and/or telephone number and/or bank account number and/or criminal records information and/or criminal organisation name and/or type of drugs and/or firearm information and/or means of communication and/or means of transportation and/or place of crime scene (*).*

(*) preferences to be indicated and substantiated. Choices can be expanded.

Feature:

- Searches can be limited to the most common search criteria or to the search criteria used in member state (e.g. some Member States might not have information on legal entities and do not wish to use them).

ANNEX II: Description of scenarios

The following embedded document contains a more detailed description of the 4 scenarios under consideration.

See Annex 6 of this report.

Annex 8: Status summary

Country	***SPOC appointment***	***Questionnaire***	***Mission***	***Mission date***
AT	completed	completed	-	-
BE	completed	completed	completed	17 Jan
BG	completed	completed	completed	5 Mar
CY	completed	completed	-	-
CZ	completed	completed	completed	6 Feb
DE	completed	completed	completed	23 Feb
DK	completed	completed	-	-
EE	completed	completed	completed	22 Mar
EL	completed	completed	-	-
ES	completed	completed	completed	16 Mar
FI	completed	completed	completed	12 Mar
FR	completed	completed	completed	20 Mar
HU	completed	completed	-	-
IE	completed	completed	-	-
IT	completed	completed	-	-
LT	completed	completed	-	-
LU	completed	completed	-	-
LV	completed	completed	-	-
MT	completed	completed	-	-
NL	completed	completed	completed	8 Mar
PL	completed	completed	completed	28 Feb
PT	completed	completed	-	-
RO	completed	completed	-	-
SE	completed	completed	completed	29 Mar
SI	completed	completed	-	-
SK	completed	completed	-	-
UK	completed	completed	completed	9 Feb

Annex 9: Folders with filled out Questionnaires and Interview Guides

Folders with final filled out Questionnaires

Provided in the form of electronic support

Folders with final filled out Interview Guides

Provided in the form of the electronic support

Annex 10: Relevant projects and systems in place

In order to better understand the context for the establishment of a possible future mechanism for the information exchange between law enforcement authorities in EU Member States, an assessment of several relevant information exchange instruments and upcoming projects is to be conducted. This will facilitate the identification of their qualities and shortcomings in the light of the needs of EPRIS and help determine whether or not a new information system is needed and which focus points are to be taken into account. The overview will thus focus on the relevant elements in different systems while at the same time taking into account how they contribute to the purpose and needs of EPRIS**.** The possibility of re-using existing structures and avoiding duplications will be considered.

When elaborating this section, previous research work and studies conducted by the European Commission as well as other institutions/bodies has been taken into account.[38]

Europol Information System (EIS)

The Europol Information System is ***a central database*** managed by Europol, storing information falling under its mandate. More specifically, it contains data related to persons who are suspected or persons regarding whom there are factual indications or reasonable grounds to believe that they will commit, have committed or participated in a criminal offence in respect of which Europol is competent.

Advantages in terms of EPRIS' purpose

- The EIS contains information on suspects and criminal offences**;**
- Whether the information to be uploaded to EIS falls under Europol's mandate, is a decision taken by the Member States. Practice shows that also non-mandate information is uploaded to the EIS. If Europol's mandate would no longer form a barrier for information that is being uploaded in EIS, it could function as an information hub for all criminal investigations related information. One idea could be to upload all law enforcement records information in EIS, but limit Europol's access to information falling within its clearly-defined mandate.
- The Europol channel is the only[39] EU channel which uses a (however non-mandatory) standardised handling code system. It is thus immediately clear which restrictions apply to the use of the information received.[40]

[38] Overview of information management in the area of freedom, security and justice, COM(2010)385 final, 20.7.2010; International Centre for Migration Policy Development and European Public Law Organisation, Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments, JLS/2009/ISEC/PR-001-F3, December 2010; European Information Exchange Model. Conclusions of the Information Mapping exercise of 2010, HOME/A3 (2011), 2.5.2011; Results of the pre-study on the need for, and the added value of, setting up a European Police Records Index System (EPRIS)

[39] Interpol is the only other channel which uses a standardised system similar to 'handling codes', by letting the Member States mention restrictions and caveats when registering information in ICIS

- The EIS contains information not only from police authorities but from a whole range of relevant law enforcement authorities, such as customs, border guards and financial crime unites. Rather than its source, it pays attention to the finality of the relevant information, which means the information has to fall within Europol's mandate.
- Member States are automatically notified of a relevant hit in EIS when information is being uploaded.
- After a hit has been produced, the actual information exchange can be conducted by liaison officers stationed at Europol.
- Numerous countries desire to strengthen the role of Europol.[41]

Disadvantages in terms of EPRIS' purpose

- The main shortcoming with regard to exchange via EPRIS is related to the fact that EIS holds information relevant for criminal investigations, but Europol's mandate is limited to organised crime, terrorism and serious crime as described in the annex of the Europol Council Decision[42]. The data in EIS is therefore equally limited to those crimes. E.g. police services investigating a cross-border non-listed crime are not able to get cross-border hit notifications of relevant information. Additionally, not all Member States contribute to EIS in an equivalent way (regarding the amount and quality of uploaded data).
- Access and the possibility to make queries in the EIS are limited in Member States.
- During missions, some Member States have clarified that the level of confidentiality of the EIS and related operations is either too stringent or too lax to allow for an efficient integration in daily workflows and information systems at national level.

SIENA

SIENA is a secure communication platform used to manage the exchange of operational and strategic crime- related information between Member States, Europol and third parties with which Europol has cooperation agreements. SIENA operates in a way that complies with all the legal requirements of data protection and confidentiality. It ensures the secure exchange **of sensitive information.**

(International Criminal Information System). However, they are less practical as those used at Europol (e.g. a limited hit/no-hit functionality). Member States often do each have their own classification system.

[40] Example:
No Handling Code is applied.
Handling Code H1 - This information must not be used as evidence in judicial proceedings without the permission of the provider.
Handling Code H2 - This information must not be disseminated without the permission of the provider.
Handling Code H3 - Other restrictions apply (followed by free text).

[41] International Centre for Migration Policy Development and European Public Law Organization, Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments, JLS/2009/ISEC/PR-001-F3, December 2010, p. 55

[42] Council Decision establishing the European Police Office (Europol), (OJ L 121 of 15.5.2009)

Advantages in terms of EPRIS' purpose

- No need for a new technical infrastructure/communication channel;
- SIENA is already used by several MS.
- Possibility to exchange information beyond Europol's mandate between Member States via SIENA.

Disadvantages in terms of EPRIS' purpose

- SIENA is deemed as difficult to use by Member States due to the conditions associated with its EU RESTRICTED accreditation.
- Currently SIENA is offered as a web based form that cannot be integrated easily in the MS ICT systems.
- Most of the activities/processes necessary to be used for EPRIS' purposes are manually driven.

Schengen Information System (SIS II)

The Schengen Information System is seen as a cornerstone of the EU's internal security and migration management strategies. It is ***a central database*** which contains alerts on certain categories of persons and objects, supplied by the Member States as described in, for the current system, in Articles 95-100 of the Convention implementing the Schengen Agreement[43]. Different law enforcement authorities may access SIS, as well as judicial authorities including those involved in criminal proceedings and visa/immigration authorities, although this access is limited to their respective legal powers. Whenever a match is found between inputted data and an existing alert in the system, the consulting party is notified of a 'hit'. Any supplementary information related to a hit may then be requested through the use of the SIRENE network (except for extradition alerts where the information is forwarded at the time of alert issue in order to facilitate validation of the incoming alert by other Member States). SIRENE stands for Supplementary Information Request at the National Entry and outlines the main task of the "SIRENE Bureaux" established in all Schengen States, which is the exchange of additional or supplementary information on alerts between the states.

Advantages in terms of EPRIS' purpose

- Alerts in SIS are inputted by different authorities. Access to SIS is however limited to the competences of the respective authorities. For police and judicial authorities this access tends to cover all the available information.
- SIS is considered user-friendly (often integrated in national systems, wide net of access points, quick dissemination/responses, permanence).
- SIRENE offices are able to exchange any useful information through a dedicated network, and are thus not limited to the information stored in SIS. SIRENE also enables a swift follow-up after a hit has been achieved.

[43] Convention of 14 June 1985 implementing the Schengen Agreement 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, 19.6.1990.

Disadvantages in terms of EPRIS' purpose

- The SIS is characterised by information on a data subject which is limited by the legal base. Due to the use of free text fields there is the risk of some end users entering low quality data. However, extensive data quality checking processes are in place. This risk will be mitigated in SIS II which is menu-driven wherever possible.
- SIS is mainly used as a border control/migration instrument (60% of alerts on persons relates to third country citizens whose entry should be refused, while 85% of alerts on objects relates to documents, e.g. lost, stolen or misappropriated identification papers, extended under SIS II with "invalidated" documents). Its use as a criminal investigations tool as envisaged by EPRIS is thus far from ideal, even though the legal base permits such use to carry out discreet or specific checks to prosecute criminal offences and prevent threats to public security. The wording of the SIS II legal base in this respect is clearer.
- SIS only contains alerts/information brought to the attention by the Member States themselves, thus overlooking data that was not deemed relevant by the uploading Member States.

Prüm Decision

The Prüm Decision[44] lays down rules for the cross-border exchange of information. It interconnects, in ***a decentralised way***, the vehicle registration, fingerprint and DNA databases of the Member States. The Prüm Decision additionally allows for the exchange of personal and non-personal data for the prevention of criminal offences and for maintaining public order and security for major events with a cross-border dimension. The comparison of DNA profiles and fingerprints operates on a hit/no hit basis, whereby law enforcement authorities may ask for personal information once a hit has been produced, through the established information exchange channels.

Advantages in terms of EPRIS' purpose

- The automated search in DNA and fingerprint databases is done on a hit/no hit basis.
- The Prüm decision seems to be one of the most efficient tools to identify criminals and solve crimes. This is due to the possibility of almost instantly knowing if a certain type of information is available in another Member State and, if so, where it is kept. Since a formal request can then be sent directly to the appropriate authority, such a facility is regarded as enormous value to investigations, gaining time and increasing efficiency.

[44] Council Framework Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L212 of 6.8.2008

Disadvantages in terms of EPRIS' purpose

- The conceptualisation of Prüm as a purely decentralised system is accountable for the fact that its architecture and implementation is time-consuming and resource-intensive.
- Whereas the purpose of EPRIS would be to query the law enforcement records of the Member States, the Prüm network allows for the automatic search of separate DNA, fingerprint and vehicle registration databases.

Customs Information System/Customs File Identification Database (CIS/FIDE)

The Customs Information System aims at an intensified and rapid dissemination of data and information between Member States' administrative authorities, to assist in the prevention, investigation and prosecution of violations of customs and agricultural law. It is set up as ***a central database***, comprising personal data. The data may be copied from CIS but only for the time necessary to achieve the purpose for which they were copied and for no longer than 10 years. Linked with CIS, Customs File Identification Database has been developed as a register of criminal investigation cases on customs matters. It enables Member States to identify other authorities that may have investigated a given person or business. Member States may enter data in FIDE from their investigation files.

Advantages in terms of EPRIS' purpose

CIS is a common computer network which increases the effectiveness of cross-border co-operation. Member States describe it as useful for investigations on suspicious persons or transports.

Disadvantages in terms of EPRIS' purpose

- FIDE serves as a tool to know whether relevant information exists in another Member State. However, it does not look at all customs information but only at information the Member States have uploaded themselves in FIDE.
- The system is limited to customs authorities, so the information from the customs' criminal investigation records cannot be used by police authorities and vice versa.
- A lack of users has been reported among Member States, which limits the number of answers received from FIDE. Other channels are therefore often used (e.g. bilateral or Europol channel).

European Criminal Records Information System (ECRIS)

According to the Council Framework Decision on the organisation and content of the exchange of information extracted from the criminal record[45] and its implementing Decision[46], ECRIS interconnects Member States' criminal record databases via the Commission's s-TESTA network. The information exchange happens in ***a decentralised way***. The Member State of conviction transmits the information to the Member State of nationality which has an obligation to store the transmitted data.

Advantages in terms of EPRIS' purpose

- Use of existing IT-infrastructure: the network developed by the Commission is used to ensure a secure information exchange.
- EPRIS could apply the EU-wide codes for offences used in the framework of ECRIS. Similarly to criminal records databases, law enforcement databases should be restructured, allocating a unified offence code to each national offence.

Disadvantages in terms of EPRIS' purpose

- Criminal records information on third country nationals is not being automatically forwarded using ECRIS. ECRIS-TCN should remedy this, but that instrument is still under consideration and has not been developed or implemented. Information on previous convictions via ECRIS can only be checked if a person was convicted in one of EU Member States and his country of nationality is within EU.
- ECRIS cannot be used to obtain information on the criminal records of legal persons (if those exist).
- Because there is no obligation to include information on disqualifications in the national criminal records database, information on disqualifications could potentially be incomplete.
- ECRIS is limited to information on criminal records. This means it cannot be used for a large number of person categories similar to the ones contained in criminal investigation records (e.g. suspects).

[45] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93/23 of 07.04.2009

[46] Council Decision of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA, OJ L 93/33 of 07.04.09

Swedish Initiative

Contrary to the information tools described above, the Swedish Framework Initiative[47] does not provide for any database or index system. Instead, it is a legal framework that ***streamlines the existing ways of information exchange***, by setting time limits and determining that conditions applicable to cross-border data-exchange should be no stricter than those regulating domestic access. The Swedish initiative complements existing instruments by regulating the exchange of information once it is known where the relevant information can be found.

Advantages in terms of EPRIS' purpose

- The Swedish initiative perfectly complements EPRIS, by regulating the "need to share", once it has been determined whether or not relevant information is available. In combination with Prüm, the Swedish Initiative and EPRIS could potentially encompass all EU law enforcement information exchange by determining if, where and how information should be shared.
- The Swedish Initiative determines strict time limits with which member states have to comply when responding to request for information (e.g. 8 hours for urgent requests). It should thus be used following a hit in EPRIS.
- Any existing communication channel (Europol liaisons, SIRENE, bilateral, etc.) may be chosen to send the information. For example, 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.

Disadvantages in terms of EPRIS' purpose

- The Swedish Initiative only regulates the actual exchange of information but does not help the Member States in informing them if and where there is relevant information.
- The Swedish Initiative has not been implemented by all Member States and is not used as much as it could be (although the latter should change once the proper instruments, such as Prüm and EPRIS, are in place).

EU level offence classification system (EULOCS)

Offence concepts differ in each of the Member States, despite approximation efforts. Because the EU approximation of offences only entails a minimum criminalisation obligation, offence concepts remain to have a different appearance throughout the Member States. With a view to overcome that obstacle, EULOCS, EU level offence classification system, is ***a reference index*** that brings together the current so-called Justice and Home Affairs substantive criminal law acquis. It functions as an EU-wide index, making it immediately clear for each Member State what constitutes an offence

[47] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L386/89 of 29.12.2006

in each Member State as opposed to behaviour that is not necessarily considered to be an offence.

Advantages in terms of EPRIS' purpose

- It is immediately clear for the requested Member State of which (national) offence a person is suspected.
- Similar to search when using the ECRIS-code, EPRIS searches could be conducted using the EULOCS code, which allows for more detailed queries.

Disadvantages in terms of EPRIS' purpose

The only existing shortcoming related to EULOCS is related to the fact that currently there is lack of awareness among EU Member States. Even though being the result of the EU feasibility study, conducted in 2008-2009, where all EU Member States were consulted, it is has not yet been visible at EU level. It is thus expected that Member States become knowledgeable about the advantages of this useful reference system while contributing to the present study. Convergence between EULOCS and UMF2 is being studied.

Annex 11: List of offences outside Europol's mandate

Originally, EULOCS was developed in the context of an EU study on the availability of crime statistics[48]. However, EULOCS is a classification system that intends to become the EU wide backbone of offence related information that can be used not only for the collection of crime statistics but also for any other type of information management and exchange.

This annex includes an extract from the original EULOCS to be able to demonstrate two lines of argumentation.

First, it supports the argument that EULOCS is fully compatible with the existing classification systems used in the EU criminal justice sphere. To that end, 7 columns are included in which it is visualised (by an 'X') which of the EULOCS categories also appear in (1) the European Criminal Records Information System (ECRIS), (2) the Eurojust and (3) Europol systems, (4) the categories found in data collection initiatives by the United Nations Office on Drugs and Crimes (UNODC), (5) European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and (6) Eurostat and finally (7) the offence labels found in the new Art. 83 TFEU.

Second, it supports the argument that the Europol offences only cover a fraction of the offences included in EULOCS. To that end, the Europol column is highlighted in yellow. Further development of an index system based on the Europol offences will inevitably reflect that restriction. Furthermore, it also shows that the more extended ECRIS still has some restrictions in light of the existing approximation based knowledge on common criminalisation in the EU.

EULOCS	**ECRIS**	**EUROJUST**	**EUROPOL**	**UNODC**	**EMCDDA**	**EUROSTAT (Focus)**	**Lissabon (Article 83 TFEU)**
CRIMES WITHIN THE JURISDICTION OF THE INTERNATIONAL CRIMINAL COURT	X						
GENOCIDE	X						
CRIMES AGAINST HUMANITY	X						
WAR CRIMES	X						
CRIMES OF AGGRESSION							

[48] Unisys and IRCP, Crime Statistics Project: Study on the development of an EU level offence classification system and an assessment of its feasibility to supporting the implementation of the Action Plan to develop an EU strategy to measure crime and criminal justice, 24.03.2010

PARTICIPATION IN A CRIMINAL ORGANISATION	X	X		X			X
OFFENCES JOINTLY IDENTIFIED AS PARTICIPATION IN A CRIMINAL ORGANISATION							
Directing a criminal organisation	X						
Knowingly participating in the criminal activities, *without being a director*	X						
Knowingly taking part in the non- criminal activities of a criminal organisation, *without being a director*	X						
OTHER FORMS OF PARTICIPATION IN A CRIMINAL ORGANISATION							
OFFENCES LINKED TO TERRORISM	X	X	X	X			X
PARTICIPATION IN A TERRORIST GROUP							
Offences jointly identified as participation in a terrorist group							
Directing a terrorist group	X						
Knowingly participating in the activities of a terrorist group, without being a director	X						
Other forms of participation in a terrorist group							
OFFENCES LINKED TO TERRORIST ACTIVITIES	X						
Offences jointly identified as linked to terrorist activities							
Public provocation to commit a terrorist offence							
Recruitment for terrorism							
Training for terrorism							
Aggravated theft with the view of committing a terrorist offence							
Extortion with the view of committing a terrorist offence							
Drawing up false administrative documents with the view of committing a terrorist offence							
Financing of terrorism	X	X					
Other offences linked to terrorist activities							
TERRORIST OFFENCES	X						
Offences jointly identified as terrorist offences							
Terrorist attacks upon a person’s life							
Terrorist attacks upon a person's physical integrity							
Terrorist kidnapping or hostage taking							
Causing extensive terrorist destruction							
Terrorist seizure of transport							
Terrorist activities related to weapons							
Terrorist release of dangerous substances, or causing fires, floods or explosions							
Terrorist interfering with or disrupting the supply of a fundamental natural resource							
Threatening to commit any of the terrorist acts listed							

Other terrorist offences							
TRAFFICKING IN HUMAN BEINGS	X	X	X	X			X
TRAFFICKING OF AN ADULT							
Offences jointly identified as trafficking of an adult							
For the purposes of labour or services exploitation	X						
For the purposes of sexual exploitation	X						
For the purposes of organ or human tissue removal	X						
Other forms of trafficking of an adult	X						
TRAFFICKING OF A CHILD							
Offences jointly identified as trafficking of a child							
For the purposes of labour or services exploitation of a child	X						
For the purposes of sexual exploitation	X						
For the purposes of organ or human tissue removal of a child	X						
Other forms of trafficking of a child							
For the purpose of recruiting child soldiers							
For the purpose of illegal adoption							
For other or unknown purposes							
SEXUAL OFFENCES	X						
SEXUAL ASSAULT	X						
Rape	X			X			
of an adult	X						
of a child	X						
Sexual Harassment	X						
of an adult							
of a child							
Indecent Exposure	X						
Other forms of sexual assault							
SEXUAL EXPLOITATION, PROSTITUTION AND PORNOGRAPHY							
Sexual exploitation							
Offences jointly identified as sexual exploitation of an adult							X
Offences jointly identified as sexual exploitation of a child	X						X
Other forms of sexual exploitation							
Soliciting by a prostitute	X						
Procuring for prostitution or sexual act	X						
Child Pornography	X	X	X				
Offences jointly identified as Child Pornography							
Possessing child pornography							
Producing child pornography							
Offering or making available of child pornography							
Distributing or transmitting child pornography							
Procuring child pornography for oneself or							

for another person							
Other offences related to child pornography							
OFFENCES RELATED TO DRUGS OR PRECURSORS	X			X	X		
OFFENCES RELATED TO DRUGS							
Cultivation							
Manufacturing							
Trafficking	X	X	X	X	X	X	X
Dealing							
Acquisition and Possession							
Consumption	X						
Other offences related to drugs							
promoting the consumption of drugs	X						
knowingly letting or renting a building or other place where public have access for the purpose of illegal consumption of drugs							
other							
OFFENCES RELATED TO PRECURSORS AND OTHER ESSENTIAL CHEMICALS					X		
Cultivation							
Manufacturing							
Trafficking							
Dealing							
Acquisition and Possession							
Other offences related to precursors							
FIREARMS, THEIR PARTS AND COMPONENTS, AMMUNITION AND EXPLOSIVES, *not committed or likely to be committed in the course of terrorist activities*	X						
ILLICIT MANUFACTURING FIREARMS	X						
FALSIFYING OR ILLICITLY ALTERING THE MARKING(S) ON FIREARMS							
ILLICIT TRAFFICKING FIREARMS		X	X				X
UNAUTHORISED ACQUISITION							
UNAUTHORISED POSSESSION OR USE	X						
OTHER							
HARMING THE ENVIRONMENT AND/OR PUBLIC HEALTH *not committed or likely to be committed in the course of terrorist activities*	X	X	X				
OFFENCES JOINTLY IDENTIFIED AS ENVIRONMENTAL OFFENCES							
Offences related to a quantity of materials or ionizing radiation	X						
Offences related to waste	X						
Offences related to a plant in which a dangerous activity is carried out							
Offences related to nuclear materials or other hazardous radioactive substances							
Offences related to protected fauna and flora species							
Offences related to habitats							
Offences related to ozone-depleting substances							
Offences related to illicit trafficking in hormonal substances and other growth	X	X	X				

promoters							
OTHER OFFENCES AGAINST THE ENVIRONMENT OR HARMING PUBLIC HEALTH (NOT-DRUG RELATED)	X						
Offences related to consumer protection							
Other offences							
OFFENCES AGAINST PROPERTY	X	X	X				
THEFT	X			X			
Theft with violence or intimidation						X	
Theft without violence or intimidation							
UNLAWFUL APPROPRIATION	X			X			
Racketeering and extortion		X	X				
Knowingly concealing or retaining property resulting from an offence							
Embezzlement, concealment of assets or unlawful increase in a company's liabilities							
Unlawful dispossession							
Other forms of unlawful appropriation							
ILLICIT DEALING IN OR CONCEALING GOODS							
Illicit trafficking in cultural goods	X	X	X				
Dealing in stolen goods	X						
Other forms of illicit dealing in or concealing goods							
CRIMINAL DAMAGE	X						
Destruction	X						
Sabotage **Smearing**	X						
Other forms of criminal damage							
CORRUPTION		X	X	X			
Offences jointly defined as corruption							
Active corruption in the public sector involving a EU public official							
Passive corruption in the public sector involving a EU public official							
Other forms of corruption							
MONEY LAUNDERING	X	X	X				X
Offences jointly identified as Money Laundering							
The conversion or transfer of property							
The illicit concealment or disguise of property related information							
The illicit acquisition, possession or use of laundered property							
Other forms of Money Laundering							
VIOLATON OF COMPETITION RULES	X						
FRAUD AND SWINDLING	X	X	X				
Offences jointly identified as fraud and swindling							
Counterfeiting and piracy products							
Forgery (i.e. Counterfeiting) and trafficking of administrative documents		X	X				
Forgery (i.e. Counterfeiting) of means of	X	X	X				X

payment							
Forgery (i.e. Counterfeiting) of cash means of payment	X			X			
Forgery (i.e. Counterfeiting) of non-cash means of payment	X						
Fraud affecting the financial interests of the European Communities	X	X					
Other forms of fraud and swindling							
Tax offences	X						
Social Security or Family Benefit Fraud	X						
Custom offences	X						
Fraudulent insolvency	X						
Other	X			X			
OFFENCES AGAINST INFORMATION SYSTEMS	X	X	X				X
Offences jointly identified as offences against information systems							
Offences against the confidentiality, integrity and availability of computer data and systems							
Computer-related offences							
Offences related to infringements of copyright and related rights							
Production, possession or trafficking in computer devices or data enabling commitment of computer related offences							
Other forms of offences against information systems							
OTHER OFFENCES AGAINST PROPERTY							
OFFENCES AGAINST LIFE, LIMB AND PERSONAL FREEDOM, *not committed or likely to be committed in the course of terrorist activities* and *other than offences against the state, nation, state symbol or public authority*	X	X	X				
CAUSING DEATH		X	X				
Intentional	X			X		X	
not further specified							
causing death at the request of the victim	X						
causing death of the own child during or immediately after birth	X						
offences related to suicide	X						
illegal abortion	X						
Unintentional	X			X			
CAUSING PSYCHOLOGICAL AND/OR BODILY INJURY							
Torture	X						
Causing psychological and bodily injury, ***other than torture***							
Causing grievous bodily injury	X	X	X	X			
Causing minor bodily injury	X						
Threatening behaviour	X						
Other							
FAILURE TO OFFER AID	X						
EXPOSING TO DANGER OF LOSS OF LIFE OR GRIEVOUS BODILY INJURY	X						
KIDNAPPING, ILLEGAL RESTRAINT AND		X	X				

HOSTAGE-TAKING							
INSULT, SLANDER AND DEFAMATION	X						
BREACH OF PRIVACY, *other than through cybercrime*							
OFFENCES AGAINST THE STATE, PUBLIC ORDER, COURSE OF JUSTICE OR PUBLIC OFFICIALS	X						
OFFENCES AGAINST THE STATE AND/OR PUBLIC AUTHORITIES							
Attempt against life or health of the head of State							
Insult of the State, nation or State symbols							
Insult or resistance to a representative of public authority							
Assault on a representative of public authority							
Unlawful impersonation of a person or an authority							
Espionage	X						
High treason	X						
Offences related to elections and referendum	X						
Obstructing of public tender procedures	X						
Obstructing or perverting the course of justice, making false allegations, perjury	X						
Abuse of function	X						
Other offences against the state and/or public authorities							
OFFENCES AGAINST PUBLIC PEACE/PUBLIC ORDER	X						
Violence during sports events	X						
Violence during international conferences							
Public abuse of alcohol or drugs, other than related to road traffic regulations	X						
Offences related to illegal gambling	X						
Disturbing public order through racism and xenophobia							
Publicly inciting to racist or xenophobic violence or hatred	X						
Denial, gross minimisation, approval or justification of genocide or crimes against humanity							
0ther offences disturbing public order through racism and xenophobia							
OFFENCES AGAINST LABOUR LAW	X						
UNLAWFUL EMPLOYMENT							
Unlawful employment *of an EU national*	X						
Unlawful employment *of a third country national*	X						
OFFENCES RELATING TO REMUNERATION INCLUDING SOCIAL SECURITY CONTRIBUTIONS	X						
OFFENCES RELATING TO WORKING CONDITIONS, HEALTH AND SAFETY AT WORK	X						

OFFENCES RELATING TO ACCESS TO OR EXERCISE OF A PROFESSIONAL ACTIVITY	X						
OFFENCES RELATING TO WORKING HOURS AND REST TIME, *other than road traffic offences*	X						
OTHER OFFENCES AGAINST RIGHTS OF THE EMPLOYEES	X						
MOTOR VEHICLE CRIME AND OFFENCES AGAINST TRAFFIC REGULATIONS, *other than theft, misappropriation and trafficking in stolen vehicles*	X						
DANGEROUS DRIVING							
DRIVING WITHOUT A LICENCE OR WHILE DISQUALIFIED	X						
FAILURE TO STOP AFTER A ROAD ACCIDENT	X						
AVOIDING A ROAD CHECK	X						
OFFENCES RELATED TO ROAD TRANSPORT	X						
OTHER OFFENCES RELATED TO VEHICLES AND ROAD TRAFFIC REGULATIONS							
OFFENCES AGAINST MIGRATION LAW	X						
OFFENCES JOINTLY IDENTIFIED AS OFFENCES AGAINST MIGRATION LAW							
Unauthorised entry, transit and/or residence	X						
Facilitation of unauthorised entry, transit and residence	X	X	X	X			
OTHER OFFENCES RELATED TO IMMIGRATION/ALIEN LAWS							
OFFENCES RELATED TO FAMILY LAW	X						
OFFENCES RELATED TO FAMILY LAW, *not further specified*							
BIGAMY	X						
FAMILY ABANDONMENT BY EVADING THE ALIMONY OR MAINTENANCE OBLIGATION	X						
REMOVAL OF A CHILD OR FAILURE TO COMPLY WITH AN ORDER TO PRODUCE A CHILD	X						
OFFENCES AGAINST MILITARY OBLIGATIONS	X						

Annex 12: Inventory of Member States' national legislations

MS	*Relevant Legislation*
BE	Police function act (law 05-08-1992) Directive commune MFO-3 des Ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative (MB 202-203, published on 2002-06-18)
BG	Law on Ministry of Interior; Ordinance on the procedure for the police criminal records
CY	Processing of Personal Data (Protection of Individuals) Law 138(I)/01
DE	Federal Data Protection Act
EE	Police and Border Guard law E-File System regulation
FI	Police Act (493/1995) Act on the Processing of Personal Data by the Police (761/2003)
FR	Code de procédure pénale Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
HU	Police Act of the Republic of Hungary, Act XXXIV. of 1994 on the Police
IT	Legge 121/198, Legge 128/2001 Privacy Code – law n.196 30/6/2003
LT	Law of Police activities
LV	Law „On Police" (04.06.1991) Criminal Procedure Law (21.04.2005) Investigatory Operations Law (16.12.1993) Personal Data Protection Law (23.03.2000) Cabinet Regulation No 391 (27.04.2010) Cabinet Regulation No 850 (14.09.2010) Punishment Register Law Cabinet Regulation No 687 (22.08.2006)
RO	Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data
SI	The Police Act
SK	Police Force č. 171/1993 Coll and special act 11bc) Act No.652/2004 and Financial administration Act 354/2011 Coll

Annex 13: Bibliography

LEGAL AND POLITICAL DOCUMENTS

- COUNCIL OF EUROPE (1950), *European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11,* (CETS no. 005, Rome, 04.11.1950)
- COUNCIL OF EUROPE (1959), *European Convention on Mutual Assistance in Criminal Matters,* (CETS no.030, Strasbourg, 20.04.1959)
- COUNCIL OF EUROPE (1981), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* (CETS no. 108, Strasbourg, 28.01.1981)
- COUNCIL OF EUROPE (1987), *Recommendation of the Committee of Ministers of the Council of Europe Regulating the Use of Personal Data in the Police Sector,* (No R (87) 15, 17.091987)
- COUNCIL OF THE EUROPEAN UNION (1995), *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* (OJ L 281 of 23.11.1995 p. 31)
- COUNCIL OF THE EUROPEAN UNION (1997), *Council Regulation (EC) No 515/97 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs or agricultural matters,* (ABl. L 82 of 22.03.1997)
- COUNCIL OF THE EUROPEAN UNION (2000), *The prevention and control of organised crime: a European Union strategy for the beginning of the new millennium,* (OJ C 124/1 of 3.05.2000)
- COUNCIL OF THE EUROPEAN UNION (2006), *Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union,* (OJ L386/89 of 29.12.2006)
- COUNCIL OF THE EUROPEAN UNION (2008), *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,* (OJ L 350/60 of 30.12.2008)
- COUNCIL OF THE EUROPEAN UNION (2008), *Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime,* (OJ L 210/1 of 06.08.2009)
- COUNCIL OF THE EUROPEAN UNION (2008), *Council Framework Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime,* (OJ L212 of 6.8.2008)

- COUNCIL OF THE EUROPEAN UNION (2009), *Conclusions on an Information Management Strategy for EU internal security (press)*, 30.11.2009
- COUNCIL OF THE EUROPEAN UNION (2009), *Council Decision establishing the European Police Office (Europol)*, (OJ L 121 of 15.5.2009)
- COUNCIL OF THE EUROPEAN UNION (2009), *Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States*, (OJ L 93/23 of 07.04.2009)
- COUNCIL OF THE EUROPEAN UNION (2009), *Council Decision of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2008/315/JHA*, (OJ L 93/33 of 07.04.09)
- EUROPEAN COMMISSION (2009), *Report on the Practical Operation of the methodology for a systematic and rigorous monitoring of compliance with the Charter of Fundamental Rights*, (COM(2009) 205 final of 29.04.2009)
- EUROPEAN COMMISSION (2005), *Communication from the Commission to the Council and the European Parliament on the mutual recognition of judicial decisions in criminal matters and the strengthening of mutual trust between Member States*, (COM(2005) 195 final of 19.5.2005)
- EUROPEAN COMMISSION (2005), *Proposal for a Council Framework Decision of 12 October 2005 on the exchange of information under the principle of availability*, (COM(2005) 475 final of 12.10.2005)
- EUROPEAN COMMISSION (2006), *Commission Communication to the European Parliament, the Council and the European Economic and Social Committee: Developing a comprehensive and coherent EU strategy to measure crime and criminal justice: An EU action Plan 2006-2010*, (COM(2006) 437 final of 07.08.2006)
- EUROPEAN COMMISSION (2009), *Communication from the Commission to the European Parliament and the Council: An area of freedom, security and justice serving the citizen*, (COM (2009) 262 final of 10.06.2009)
- EUROPEAN COMMISSION (2009), *Legislative package establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, (COM(2009) 292 final of 24.06.2009)
- EUROPEAN COMMISSION (2010), *Communication from the Commission to the European Parliament and the Council: Overview of information management in the area of freedom, security and justice*, (COM(2010)385 final of 20.7.2010)
- EUROPEAN COMMISSION (2010), *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A comprehensive approach on personal data protection in the European Union*, (COM(2010) 609 final of 4.11.2010)
- EUROPEAN COMMISSION (2010), *Pre-study on the need for, and the added value of, setting up a European Police Record Index System (EPRIS), Main findings, HOME/A3 (2011)*, 19 04 2011

- EUROPEAN COMMISSION (2010), *Action Plan implementing the Stockholm Programme*, (COM(2010) 171 final of 20.4.2010).
- EUROPEAN COMMISSION (2011), *European Information Exchange Model. Conclusions of the Information Mapping exercise of 2010*, HOME/A3 (2011), 2.5.2011
- EUROPEAN COUNCIL (1999), *Tampere Presidency Conclusions,* (SN 200/1/99 REV 1)
- EUROPEAN COUNCIL (2000), *Charter of Fundamental Rights of the European Union,* (OJ C 364/1 of 18.12.2000)
- EUROPEAN COUNCIL (2004), *The Hague Programme: strengthening freedom, security and justice in the European Union*, (OJ C 53/11 of 03.03.2005)
- EUROPEAN COUNCIL (2004), *Declaration on Combating Terrorism*, (Brussels, 25.03.2004)
- EUROPEAN DATA PROTECTION SUPERVISOR (2010), *Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and on the proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty,* (5039/10, 07.01.2010)
- EUROPEAN DATA PROTECTION SUPERVISOR (2010), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council - "Overview of information management in the area of freedom, security and justice",* (Brussels, 30.09.2010)
- *Convention of 14 June 1985 implementing the Schengen Agreement 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,* 19.6.1990
- *Treaty establishing a Constitution for Europe*, (OJ C 310 of 16.12.2004)
- *Treaty on European Union* (Maastricht treaty), (OJ C 191 of 29.07.1992)
- *Treaty of Amsterdam*, (OJ C 340 of 10.11.1997)
- *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007,* (OJ C 306 of 17.12.2007)

CASE LAW

- EUROPEAN COURT OF HUMAN RIGHTS *Hatton and Others v. UK*, (2001), Application no. 36022/97, Judgment of 2.10.2001.
- EUROPEAN COURT OF HUMAN RIGHTS, *S and Marper v. UK* (2008), Application no 30562/04 and 30566/04, Judgment of 04.12.2008

- EUROPEAN COURT OF JUSTICE, (C-524/06) *Heinz Huber v Bundesrepublik Germany*, Judgment of 29 January 2008

LITERATURE

- CRAIG P. & DE BURCA G (2008) *EU Law: Text, Cases and Materials,* 4the edition, Oxford: Oxford University Press
- INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT AND EUROPEAN PUBLIC LAW ORGANISATION, *Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments,* JLS/2009/ISEC/PR-001-F3, December 2010.
- JAIN A.K., BOLLE R. & PANKANTI S., EDITORS (1999), *"Biometrics Personal identification in networked society",* Kluwer academic publishers, p. 16
- JOUTSEN, M. (2006) *The European Union and Cooperation in Criminal Matters: the Search for Balance,* HEUNI nr.25, 2006
- PRADEL, J. & CORSTENS, G. (2002)*, European Criminal Law,* The Hague: Kluwer International
- TABASSI E., WILSON C.L. & WATSON C. (2004), *Fingerprint Image Quality,* National Institute of Standards and Technology (NIST)
- UNISYS (2006), *Research, Global Study on the Public's Perceptions about Identity Management*, May 2006
- UNISYS AND IRCP (2010), *Crime Statistics Project: Study on the development of an EU level offence classification system and an assessment of its feasibility to supporting the implementation of the Action Plan to develop an EU strategy to measure crime and criminal justice,* 24.03.2010
- UNISYS (2011), Project Inception Report, Contract HOME/2010/ISEC/PR/068-A3 *Feasibility Study: on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records Index System*, Version 2.00 of 2011
- UNISYS (2012), Project Interim Report, Contract HOME/2010/ISEC/PR/068-A3 *Feasibility Study: on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records Index System*, Version 2.01 of 2012
- VACCA J. (2007), *Biometric technologies and verification systems,* Butterworth Heinemann, pp. 287-316
- VERMEULEN, G., VANDER BEKEN, T., DE BUSSER, E. & DORMAELS, A. (2002), *Blueprint for an EU Criminal Records Database,* Antwerp: Maklu
- VERMEULEN, G. & DE BONDT, W., "EULOCS (2009), *The EU level offence classification system"* in IRCP-series 35, p.112
- VERMEULEN, G., DE BONDT, W. & RYCKMAN, C. (eds.) (2011), *Rethinking international cooperation in criminal matters in the EU,* Antwerp, Maklu, p.620

- VERMEULEN, G., VANDER BEKEN, T., VAN PUYENBROECK, L. & VAN MALDEREN, S. (2005), *Availability of law enforcement information in the European Union*, Antwerp, Maklu, p.110
- VERMEULEN, G. (2008), *Mutual recognition, harmonisation and fundamental (procedural) rights,* In MARTIN, M. (ed.) (2008) *Crime Rights and the EU. The future of police and judicial cooperation*, London: Justice, pp. 89-104
- XANTHAKI, H (2002), C*ooperation in Justice and Home Affairs*, in J. Gower (ed.), (2002) *European Union Handbook*, London-Chigaco: Fitztroy Dearborn Publishers, pp. 234-242